

THE PROMISES AND PERILS OF EMERGING TECHNOLOGIES FOR CYBERSECURITY

HEARING

BEFORE THE

COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

MARCH 22, 2017

Printed for the use of the Committee on Commerce, Science, and Transportation



U.S. GOVERNMENT PUBLISHING OFFICE

28–382 PDF

WASHINGTON : 2018

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

JOHN THUNE, South Dakota, *Chairman*

ROGER F. WICKER, Mississippi	BILL NELSON, Florida, <i>Ranking</i>
ROY BLUNT, Missouri	MARIA CANTWELL, Washington
TED CRUZ, Texas	AMY KLOBUCHAR, Minnesota
DEB FISCHER, Nebraska	RICHARD BLUMENTHAL, Connecticut
JERRY MORAN, Kansas	BRIAN SCHATZ, Hawaii
DAN SULLIVAN, Alaska	EDWARD MARKEY, Massachusetts
DEAN HELLER, Nevada	CORY BOOKER, New Jersey
JAMES INHOFE, Oklahoma	TOM UDALL, New Mexico
MIKE LEE, Utah	GARY PETERS, Michigan
RON JOHNSON, Wisconsin	TAMMY BALDWIN, Wisconsin
SHELLEY MOORE CAPITO, West Virginia	TAMMY DUCKWORTH, Illinois
CORY GARDNER, Colorado	MAGGIE HASSAN, New Hampshire
TODD YOUNG, Indiana	CATHERINE CORTEZ MASTO, Nevada

NICK ROSSI, *Staff Director*

ADRIAN ARNAKIS, *Deputy Staff Director*

JASON VAN BEEK, *General Counsel*

KIM LIPSKY, *Democratic Staff Director*

CHRIS DAY, *Democratic Deputy Staff Director*

RENAE BLACK, *Senior Counsel*

CONTENTS

	Page
Hearing held on March 22, 2017	1
Statement of Senator Thune	1
Prepared statement from Professors Scott Shackelford and Steve Myers, Indiana University	74
Prepared statement from Larry Clinton, President and CEO, Internet Security Alliance	81
Prepared statement from Theresa Payton, CEO, Fortalice Solutions LLC ..	87
Statement of Senator Nelson	3
Statement of Senator Wicker	45
Statement of Senator Cantwell	49
Statement of Senator Inhofe	51
Statement of Senator Schatz	53
Statement of Senator Markey	55
Statement of Senator Peters	57
Statement of Senator Cortez Masto	59
Statement of Senator Udall	61
Statement of Senator Fischer	63
Statement of Senator Hassan	64
Statement of Senator Blumenthal	66
Statement of Senator Cruz	72

WITNESSES

Caleb Barlow, Vice President, Threat Intelligence, IBM Security	4
Prepared statement	6
Venky Ganesan, Managing Partner, Menlo Ventures; and Chair, National Venture Capital Association	10
Prepared statement	12
Steve Grobman, Intel Fellow and Chief Technology Officer, Intel Security Group	20
Prepared statement	21
Malcolm Harkins, Chief Security and Trust Officer, Cylance Inc.	28
Prepared statement	30
Hon. Eric Rosenbach, Former DOD Chief of Staff and Former Assistant Secretary of Defense for Homeland Defense and Global Security	42
Prepared statement	44

APPENDIX

Letter dated March 22, 2017 to Hon. John Thune and Hon. Bill Nelson from Marc Rotenberg, President, EPIC; and Caitriona Fitzgerald, Policy Director, EPIC	91
Response to written questions submitted to Caleb Barlow by:	
Hon. John Thune	95
Hon. Todd Young	97
Hon. Edward Markey	98
Hon. Tammy Duckworth	98
Response to written questions submitted to Venky Ganesan by:	
Hon. John Thune	99
Hon. Jerry Moran	100
Hon. Edward Markey	101
Hon. Tammy Duckworth	101

IV

	Page
Response to written questions submitted to Steve Grobman by:	
Hon. John Thune	102
Hon. Edward Markey	105
Hon. Tammy Duckworth	106
Response to written questions submitted to Malcolm Harkins by:	
Hon. John Thune	108
Hon. Edward Markey	110
Hon. Tammy Duckworth	110
Response to written questions submitted to Hon. Eric Rosenbach by:	
Hon. John Thune	111
Hon. Bill Nelson	113
Hon. Edward Markey	113
Hon. Tammy Duckworth	114

THE PROMISES AND PERILS OF EMERGING TECHNOLOGIES FOR CYBERSECURITY

WEDNESDAY, MARCH 22, 2017

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m. in room SD-106, Dirksen Senate Office Building, Hon. John Thune, Chairman of the Committee, presiding.

Present: Senators Thune [presiding], Wicker, Cruz, Fischer, Moran, Sullivan, Heller, Inhofe, Capito, Gardner, Young, Nelson, Cantwell, Klobuchar, Blumenthal, Schatz, Markey, Booker, Udall, Peters, Hassan, and Cortez Masto.

OPENING STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

The CHAIRMAN. Good morning. As chairman, I've made it a priority for this committee to focus on emerging technologies. We've held some of the first hearings in Congress on artificial intelligence, self-driving vehicles, Internet of Things, and augmented reality. Today, we'll continue this practice, but this time, we'll be focusing on the potential benefits and sometimes risks that certain emerging technologies have on cybersecurity.

As my fellow committee members know well, cybersecurity is a topic that comes up at almost every hearing that we hold. The cutting edge technologies we're exploring today are fundamentally transforming how people and businesses connect as well as the creation and transmission of information.

Emerging technologies such as artificial intelligence, block chain, and quantum computing, as well as the flourishing Internet of Things offer innovative approaches for combating future cyber threats, but also present new risks. As threats continually evolve, flexible and innovative approaches will be required to protect businesses, critical infrastructure, and individual citizens.

This hearing will explore the enormous potential of these fields to revolutionize the cybersecurity arena and grow our economy. For example, by 2020, the estimated number of connected devices making up the Internet of Things may exceed 50 billion. Furthermore, a World Economic Forum report predicts that 10 percent of global gross domestic product will be stored on blockchain technology by 2027.

Artificial intelligence, or AI, will increasingly allow computers to mimic cognitive functions associated with humans. And, as described in a recent cover story in *The Economist*, quantum compu-

ting's untapped potential will be capable of handling complex problems that today's computers cannot solve.

Even with all of their promise, these technologies also have the potential to create new security risks. For example, nefarious hackers can use AI to identify cyber vulnerabilities and victims faster. Future quantum computers could break our current encryption standards with ease.

Federal agencies under the Committee's jurisdiction, such as the Department of Commerce, the National Science Foundation, the White House Office of Science and Technology Policy, and NASA, in partnership with academia and industry, are focused on research and the development of standards to ensure the U.S. remains the leader in these fields. Our committee has been supportive of prioritizing such work due its national and economic security benefits.

The recently enacted bipartisan American Innovation and Competitiveness Act, sponsored by Senators Gardner, Peters, Nelson, and myself, charged our science agencies to research future cybersecurity needs. In particular, the law directed the Commerce Department's National Institute of Standards and Technology to work with stakeholders to identify cryptography standards that future computers will not be able to break, and directed NSF to focus research on cybersecurity and human-computer interactions.

In addition, the bipartisan Cybersecurity Enhancement Act of 2014, which I co-sponsored with then Chairman Rockefeller, included important provisions for cybersecurity research, workforce development, and standards. It authorized NIST's continued efforts to develop the voluntary Framework for Critical Infrastructure Cybersecurity and the National Initiative on Cybersecurity Education, as well as the NSF's successful Cybercorps scholarship program. In fact, Dakota State University, which is located in my home state of South Dakota, is an active participant in this program.

Our nation faces an array of evolving cyber threats to our personal data, access to online services, and critical infrastructure. To be clear, cybersecurity is not solely a technology issue. Also, while there is no silver bullet solution to cybersecurity risks, I believe promoting public-private partnerships on risk management, foundational research, and a robust cyber workforce are essential to combating these challenges. That is why I am excited to continue our Committee's discussion on cybersecurity by looking toward the future.

The companies represented at today's hearing are driving innovation. They have employed machine learning to identify new threats, conducted research that may soon unlock the commercial potential of private blockchains and quantum computing, and launched new tech startups that create jobs and grow the economy.

And, Mr. Rosenbach, thank you for your dedicated service at the Defense Department.

Cybersecurity will continue to be a priority for this committee. In fact, Senator Gardner and I will be sending letters to newly confirmed Commerce Secretary Ross and Transportation Secretary Chao urging them to prioritize the cybersecurity of Federal systems. As the heads of their respective departments, they have an

opportunity to improve the effectiveness of cybersecurity programs. In addition, I look forward to working with Senators Schatz, Risch, and Cantwell on potential legislation to ensure that small businesses fully benefit from the NIST Cybersecurity Framework.

I want to thank all of our witnesses for being here today. I look forward to hearing your testimony. I will now turn it over to Senator Nelson for his opening remarks.

**STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA**

Senator NELSON. Thank you, Mr. Chairman, and in order to condense so we can get on with our witnesses and not to be repetitive, let me just point out a couple of things.

Of course, this committee has a lot of things that involve cybersecurity, everything from commercial aviation to the driverless cars, and we are in this era in which cyber attacks keep coming, and the advent of technology, one of which we were dealing with in a classified session this morning, is going to almost be like whack-a-mole. You hit them here and they pop up over here, because technology is going to advance.

And then with the rapid commercialization of the Internet of Things, it provides consumers with many, many benefits, but also provides hackers with a multitude of opportunities. You mentioned, Mr. Chairman, artificial intelligence and quantum computing. That could greatly enhance our cyber defense capabilities, but put it in the bad guy's hands and it makes it much more difficult for us, much more difficult to detect threats and risks to things like economic and physical well-being.

Blockchain technology, which has proven successful in securing financial transactions, could be used to secure all kinds of sensitive data and information. I hope that we can learn more from you all today about this.

Obviously, we are all concerned about cybersecurity, I hope. Or is it, with regard to a lot of Americans, out of sight, out of mind, until they get hit, such as the privacy of their own information, the hack of their bank account? What about their insurance company, and what about power grids?

According to the intelligence community's assessment recently, we know that the Russian hackers at the president of Russia's direction used a series of relatively simple cyber attacks to try to influence our last Presidential election, striking at the very core of how we operate this democracy. So because what we're going to discuss today, that some of these technologies can be used against us in a cyber attack, I'd like to know how Russia, China, and the other adversaries might use these technologies to disrupt our economy, if you all can say this in this open session.

How might the Russian hackers, which seem to be the most technically proficient—how might they use the Internet of Things to hack our most vulnerable systems? How might blockchain technology be used to secure sensitive data or disguise illicit activity? How might quantum computing and artificial intelligence improve or undermine the security of everyday Americans? These are questions I'd like you to address.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Nelson.

As I said, we've got a great panel today, and we look forward to hearing from each of you. I'm going to start by introducing the folks on my left and your right: Mr. Caleb Barlow, who is Vice President of Threat Intelligence for IBM Security; Mr. Venky Ganesan, Chair, National Venture Capital Association and a Partner at Menlo Ventures; Mr. Steve Grobman, who is the Chief Technology Officer and Intel Fellow at Intel Security; Mr. Malcolm Harkins, the Chief Security and Trust Officer at Cylance Corporation; and the Honorable, as I said earlier, Eric Rosenbach, Former Chief of Staff, Office of the Secretary of Defense, and former Assistant Secretary of Defense for Homeland Defense and Global Security.

It's great to have you all here. Thanks so much for making yourselves available to share with us your thoughts. And if you could, as you share your opening statements, confine them orally as close to 5 minutes as possible. Any additional information or material you want, we can get it into the record. But that will maximize the opportunity for members to ask questions.

So we'll start with Mr. Barlow.

Please proceed.

**STATEMENT OF CALEB BARLOW, VICE PRESIDENT,
THREAT INTELLIGENCE, IBM SECURITY**

Mr. BARLOW. Chairman Thune, Ranking Member Nelson, distinguished members of the Committee, thank you for the opportunity to appear here today before the Committee to discuss this important topic.

I am here representing IBM Security, where I lead the company's global threat intelligence business, which helps clients around the world find, manage, and remediate cyber attacks. We also help clients in responding to cybersecurity incidents, from guidance on how to manage regulatory and compliance requirements to incident response services. Last year, we significantly expanded IBM's incident response capabilities with a \$200 million investment, which included us opening the IBM X-Force Command Center in Boston, Massachusetts, which is the world's first at-scale cyber simulation range for the private sector.

Now, from my vantage point, working in one of the largest security intelligence operations in the world, IBM manages 35 billion security events every day on behalf of our clients. I see a change in the threat landscape unfolding before me.

Until now, just about everything we've heard about involves the exfiltration of data. A bad guy breaks into a system, gets access to information, downloads it, and then extorts that for profit or influence. But what if rather than stealing the data or holding it hostage with ransomware, what would happen if the cyber criminal changed it? Think about how much we rely on data from computers and just trust that it's accurate. Now, if trust is broken, even the smallest of actions can have tectonic implications, because the natural human tendency is to run from areas of risk to areas of safety.

Today, I would like to discuss greater collaboration in sharing cyber threat data between the public and the private sector. We're seeing security attacks and techniques continue to evolve, and why there's a lot of focus on nation-state activity, a United Nations re-

port estimated that 80 percent of attacks are actually driven by highly organized and ultra sophisticated criminal gangs.

The most sophisticated thieves operate like well-oiled businesses. They collaborate and share expertise on a global scale. They operate with anonymity and seemingly outside the reach of the law. Cyber crime has grown rapidly due to its organization and collaboration to become a significant societal issue. Cyber crime is now estimated to be one of the largest illegal economies in the world, costing the global economy—now get this—more than \$445 billion annually. Now, to put this into perspective, \$445 billion is greater than the GDP of more than 160 nations, including Ireland, Finland, Denmark, and Portugal, among many others.

What we need to do if we are truly going to stop this is change the economics for the bad guys. You see, we've reached a point where new actions and strategies are required. The scale and pace of threat information sharing needs to be accelerated between the public and the private sector. Threat sharing is only actionable when it happens with speed.

Security vendors, governments, and other organizations need to open up their arsenal of information on threats, the types of threats, where they're coming from, and how they work, and share them openly and at scale. Simply put, we must democratize threat intelligence data. Governments need to support threat sharing by declassifying their own data at default and with speed, not measured in months or even years like it is today, but measured in hours and minutes.

You see, by uncovering criminals' devices closer to real time, we foil their schemes. By consistently keeping pace with threat intelligence and using it to outmaneuver the criminals, we gradually make cyber crime not pay. We change the economics for the bad guys.

Now, new technologies such as cognitive have enormous potential to radically reduce cyber crime while also helping to close a cybersecurity skills gap and create new collar jobs. Now, this cybersecurity skills gap is likely to exceed 1.5 million open and unfilled cybersecurity jobs by 2020.

IBM is bringing cognitive computing to the war on cyber crime. Watson for Cyber Security sorts through, analyzes, and understands massive amounts of structured data and unstructured data that can overwhelm security professionals.

Now, true cognitive systems and technologies, like IBM Watson, understand the nuances of language and threat data, and they offer remediation actions and strategies, all with the necessary speed to stay ahead of advance threats. Cognitive systems are those that can reason and learn, as compared to traditional systems that are programmed. In security terms, cognitive systems can understand that a bug is a software defect and not an insect.

While intelligent cybersecurity systems are fast advancing, as demonstrated in cognitive computing, private and public organizations need a new mindset, one that democratizes, declassifies, and shares threat data by default and with speed.

Thank you for the opportunity to appear here before the Committee today. I look forward to your questions.

[The prepared statement of Mr. Barlow follows:]

PREPARED STATEMENT OF CALEB BARLOW, VICE PRESIDENT, THREAT INTELLIGENCE,
IBM SECURITY

Chairman Thune, Ranking Member Nelson, and distinguished Members of the Committee, I am pleased to appear before you today to discuss how emerging technologies can help American companies more effectively defend themselves against cyberattacks. In my testimony, I will focus on the state of cybercrime, the importance of sharing data on cyber threats, and how emerging technologies, such as blockchain and cognitive systems that learn and reason, help dramatically reduce cybercrime while also closing the looming cybersecurity skills gap.

The State of Cybercrime

Before discussing emerging security technologies, it's important to describe the current state of cybercrime. Today, just about everything we hear about involves the exfiltration of data. A cybercriminal breaks into a system, gets access to information, downloads that data and extorts it for profit or influence. Over 2 billion records were stolen last year alone. And in 2015, over 100 million people—most of whom were Americans—had their healthcare records stolen.¹

From my vantage point working in one of the largest security intelligence operations in the world—IBM manages 35 billion security events *per day* for our clients—I see not only how many records are being stolen, but other changes that are unfolding. For example, it's not just the amount of records being stolen, but what cybercriminals are doing with the information. Rather than just stealing the data to profit from it, what would happen if a cybercriminal changed it? What would happen if they manipulated a financial record or rerouted a supply chain?

These types of attacks are emerging. Before the 2016 Summer Olympic games, a group of hackers who call themselves “Fancy Bear” accessed athletes’ data in the World Anti-Doping Agency’s database. They then released sensitive data; for example, they listed athletes who were given permission to use otherwise banned substances such as certain types of asthma medication.

But what is particularly alarming is that this hacker group allegedly did more than just steal and release data. According to the World Anti-Doping Agency, the hackers also made changes to the data prior to releasing it, in an attempt to swing public opinion.

By breaking trust, even the smallest of actions can have tectonic implications. For example, if cybercriminals manipulate the data consumers have come to inherently trust—from the financial reporting of the companies they invest in to their healthcare records—we move beyond stolen information and money to an even more damaging issue: a loss of trust. This, of course, could have many damaging ramifications. Imagine the uncertainty you would face regarding the soundness of your investments if you read that a cybercrime gang had manipulated the financial records of companies in your portfolio.

We are seeing security attacks and techniques continue to evolve, and it's important to understand where they are originating from, not necessarily geographically but from an economic and sociologic perspective. The United Nations estimates that 80 percent of cybercrime is from highly organized and ultra-sophisticated criminal gangs.² It is now estimated to be one of the largest illegal economies in the world, costing the global economy more than \$445 billion a year.³ To put this in perspective, \$445B is greater than the GDP of more than 160 different countries, including Ireland, Malaysia, Finland, Denmark, and Portugal, among many others.⁴

The most sophisticated thieves operate like a well-oiled global business. They build development tools and collaborate on software. They share knowledge about targets and vulnerabilities. In fact, each successful attack proliferates the skills, tools and ecosystem because hackers often reuse malware and other vulnerabilities that they know are proven to work. Think of it as on-the-job training.

They operate on a regimented schedule like many legitimate companies; their employees work Monday through Friday and take the weekends off. We know this because our security researchers see repeated spikes of malware launched on Fridays as hackers head home for the weekend. On Monday, the criminals regroup to see how well things went.

¹ See: IBM Security Intelligence by Caleb Barlow, Attackers Shift Sights from Retail to Health Care in 2015 <http://ibm.co/IVpruus>

² United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, February 2013

³ Net Losses: Estimating the Global Cost of Cyber Crime, Center for Strategic and International Studies, June 2014

⁴ See: <http://statisticstimes.com/economy/countries-by-projected-gdp.php>

They collaborate and share expertise on a global scale via the “Dark Web”—a term used to describe the anonymous Internet where identity-masking tools enable criminals to operate without detection. Networks of thieves steeped in both IT and business skills work together to steal intellectual capital to damage businesses, and take your money.

The Dark Web is where these criminals build and peddle attack software to steal data from businesses and other institutions. Their cohorts can purchase everything online from base-level attack platforms to premium versions, which might offer a gold, silver and bronze-level of service—and even a money-back guarantee if they don’t get a successful hack. There are different products and prices, along with ratings and reviews of the “merchants.” If you buy a hack from a “reputable criminal” with good ratings, you are far more likely to purchase a hack that is going to work.

Another major trend in cybercrime involves the Internet of Things. In our increasingly interconnected world, the devices, the data they produce and use, and the systems and applications that support them, are all potential attack points for malicious actors. Unlike a traditional computer, these IoT devices often operate without human supervision. They can be deployed for an extended lifetime and often lack simple methods to update and patch their software, which leads to poor security. Worse yet, to ease the deployment of these IoT devices, many often ship with minimal security controls, default user ID’s and passwords that are never updated by the end user, making them easy targets for an attacker.

IoT devices are accumulating massive amounts of personal and sensitive data, like voice searches, GPS locations, and heart rate readings. If the data isn’t managed and secured, its exposure can lead to a loss of privacy and data ownership. This makes the security of the data, how it’s created, used and deleted extremely important.

Simply put, if a device connects to the internet, consumers need to understand not only what data it collects and how it is used, they must also have a way to maintain and update its security for the usable lifetime of the device.

Battling Cyber Crime via Threat Sharing

So how do we stop this? Cybercrime rings operate with anonymity and often seemingly outside the reach of the law. What we need to do is change the economics for the bad guys.

Our response to cybercrime needs to be similar to how we manage a healthcare pandemic. Sars, Ebola, Bird Flu, Zika—what is the top priority when handling an outbreak? It is knowing where infections are occurring and how they are being transmitted. First responders, physicians, hospitals, governments and the private sector all share information rapidly and openly. This is a collective and altruistic effort to stop the spread of sickness in its tracks, and then rapidly get the word out on transmission modality so that anyone not infected can protect themselves.

Unfortunately, this is not what we see today in the event of a cyberattack. Organizations are much more likely to keep the attack to themselves because of a perceived risk to their reputation. When a major breach is publicly revealed, typically all that is reported (by the media) is how many records were stolen. Even if a company makes a disclosure, rarely do organizations talk about *how* they were infected because they are worried about the risk of litigation or regulation.

Adding to the problem, many security vendors see threat data as an opportunity for profit—something of value to be shared only with high-paying customers and used for competitive advantage. And many government agencies continue to operate with Cold War-era strategies, when keeping critical information hidden from a major adversary was paramount. But in today’s world, with an asymmetric enemy that operates anywhere and with impunity, keeping government information secret can work against us. Governments, too, need to disclose cyber threat indicators, vulnerabilities, breaches and hacking schemes, when appropriate, much faster. We call this concept the “default declassification of threat data at speed.”

The good news is that we are seeing signs of progress in this area. The enactment of the Cybersecurity Information Sharing Act of 2015 (CISA), for example, was an important and helpful step forward, and we have seen progress in our discussions and work with various government agencies on sharing cyber threat data. But the scale and pace of information sharing needs to be accelerated.

Cyber threat sharing is only actionable when it happens with speed, but most governments are still keeping that data confidential for extended periods of time.

As a result, we’ve reached a point where new actions and strategies are required. Security vendors, governments and other organizations need to open their arsenal of information on threats—the types of threats, where they are coming from, how they work—and share them openly, at scale and without significant financial remuneration.

neration. Simply put, we must democratize threat intelligence data to compete with cybercriminals at their own game.

By uncovering criminals' devices closer to real time, we foil their schemes. We analyze and break their plans, and share their methods with the potential victims and general public a lot sooner than the adversaries expect. By consistently keeping pace with threat intelligence and using it to out-manuever the criminals, we gradually make cybercrime not pay. We change the economics for the bad guys.

And if it does not pay, what's the motivation to do it in the first place?

To begin addressing some of the barriers to real time threat sharing and improve the sharing ecosystem, IBM supported the enactment of CISA. However, even before CISA became law, IBM took the initiative to practice what we are preaching, to share our data on cyberthreats. In 2015, IBM opened one of the largest treasure troves of threat data in the world and created the IBM X-Force Exchange. We put it all on the Internet for free. IBM published nearly 700 terabytes of actionable threat data from around the globe, including real-time indicators of live attacks, which can be used to defend against cybercrimes. We keep publishing, every day, every hour.

Battling Cybercrime with Cognitive and Blockchain Technology

So how can we democratize threat data while reducing attribution risk to governments and private institutions?

This is where emerging technologies can play a big role in cybersecurity. Cognitive security technologies, for example, has enormous potential.

The number of risks and events is growing exponentially, and security operations teams are struggling to keep up with the volume. The threat landscape is changing rapidly, with the sophistication and numbers of threat variants becoming too great to keep pace with or stay ahead of using traditional approaches. The repercussions of incidents and breaches are increasing, with the financial costs and risks growing rapidly.

At the same time, many organizations are faced with a dearth of security experts with the right skills. These different factors make it difficult for organizations to maintain the healthy digital immune systems they need to protect themselves and are driving the need for new cognitive security technologies.

Specifically, we need new technologies that can serve as a cognitive security assistant to analyze massive amounts of data to make recommendations on remediation actions with much greater speed and precision.

To highlight the amount of security information available today, there are about 60,000 security blogs per month and 10,000 security reports per year.⁵ We estimate that organizations are spending \$1.3 million a year dealing with false positives alone, wasting nearly 21,000 hours.⁶ Cognitive security technologies can make a huge difference by helping security professionals keep up with all this information and extract value from it with greater speed and accuracy.

Last month, IBM launched a cognitive security technology called Watson for Cyber Security. About 50 organizations—Fortune 500 companies across all major industries—are now using Watson to fight cybercrime.

The scale of what Watson is doing is enormous. In less than a year, Watson for Cyber Security has analyzed more than 1 million security documents on the Internet. It is now analyzing 15,000 security documents *per day*—amounts that no army of people alone could ever process.

What is even more significant than the scale of the data being analyzed, is what cognitive security technologies, such as Watson, can do with this sea of information. Specifically, true cognitive security technologies are systems that learn versus systems that are programmed. They can scour unstructured data across the Internet—the blogs and reports, media articles, social media, and many other sources—that were previously inaccessible by traditional security tools.

Cognitive systems can be trained to understand imprecise human language in those documents—for example, understanding that in security terms a “bug” is a software defect and not an insect.

Watson for Cyber Security is the first cognitive technology that is doing all of this. Our early findings are that Watson's capabilities are 60-times faster than complex manual analysis, with 10-times more actionable indicators to uncover new threats.⁷

⁵ See: Watson for Cyber Security: Shining a light on human generated data, August 2016—<http://ibm.co/2mXuZj7>

⁶ *The Cost of Malware Containment*, by Ponemon Institute, January 2015

⁷ IBM Watson for Cyber Security Beta Testing Results

It is also important to underscore that cognitive technologies like Watson do not replace people, but help them to be more productive, precise and efficient in defending their organizations from cyberattacks.

At the same time, they will help bridge a looming skills gap—an estimated 1.5 million unfilled security jobs by the end of this decade—by making the existing security workforce more effective and efficient.

Cognitive technologies also can help create new jobs. At IBM, for example, we’re now tapping professionals who may not have a traditional college degree, but who have the needed skills and aptitude to help us in a variety of disciplines, including cybersecurity. We refer to these new professionals as “new collar” workers, who may join an organization, for example, with base-level security skills from a P-Tech school or with an Associate’s Degree.

Cognitive security technologies like Watson can help these “new collar” workers by providing them with much greater levels of security analysis and insights. Essentially, with cognitive security products, new collar employees can be paired with technology that is like the equivalent of a highly seasoned and experienced human security analyst, but one who can examine massive amounts of data at incredible speeds.

New collar jobs are one way to help reduce the security skills gap, but we also need institutions of higher education to expand their cybersecurity curricula. We need more choices for earning cybersecurity degrees and more students in the pipeline. We also need to focus on ways to develop more female experts in this field, as women represent only about 10 percent of today’s cybersecurity workforce.⁸

At IBM, we’re also looking at other ways to help our new collar and traditional security employees alike to benefit from cognitive security. One example is our new research project, code named Havyn, which brings a voice to cognitive security.

Havyn is a voice-powered security assistant that can interact verbally with security analysts in real-time on a variety of topics, from information on new threats, to data on an organization’s security posture.

Havyn creates a “second-screen experience” for security analysts. It works in the background on command, pulling data from different security tools and sources, and brings the relevant information to the surface for further investigation by human analysts.

Voice-powered tools like Havyn can greatly expand the value of cognitive security intelligence sources like Watson. Just think of Watson for Cyber Security as the brain of the Security Operations Center, and think of Havyn as bringing a voice to the brain, making Watson’s expertise even more valuable.

Blockchain is another important example of emerging technology.

Blockchain is a technology for a new generation of transactional applications that helps establish security, trust, accountability and transparency. One of the key capabilities of blockchain is the ability to maintain a record of the history of all transactions in a way that cannot be manipulated.

Not only is it inherently more secure than other protocols, but blockchain has the potential to be used by multiple parties to share cyber-threat intelligence in a way that maintains the reputation of the source of the data without revealing the identity of the source. Governments and private institutions can combine data into threat feeds that ensure transactional integrity and maintain reputation, but without identifying the contributor.

Blockchain also has potential security benefits for IoT where supply chain integrity is critical. Although there may be dozens of parties involved in an IoT supply chain, a Blockchain can ensure transactional integrity and visibility of logistical and quality metrics from manufacturer to point of use.

Blockchain has inherent qualities that provide trust and security, but, to fulfill its promise, the core technology must be further developed using an open source governance model to make it deployable on a grand scale. The Federal Government must invest in scientific research to accelerate progress. The National Institute of Standards and Technology can help shape standards for interoperability, privacy and security. And government agencies can become early adopters of blockchain applications. In addition, government has a key role to play in certifying the identities of participants in blockchain-based systems.

Conclusion

Cybercrime is one of this generation’s most vexing societal problems. As with all historic societal challenges, it requires radical change at great speed.

The public and private sector need to collaborate on a much deeper level to make the sharing of cyberthreat data a standard practice. This level of interaction and

⁸2015 report by (ISC)2

sharing will result in highly organized cybercrime fighting to thwart the massive collaboration of cybercriminals today.

We need the partnership to incubate, develop, and institute emerging security technologies such as cognitive systems and blockchain. We need higher education institutions to also step up in cultivating a new generation of security experts for our workforce.

In the process, we will not only chip away at cybercrime, but radically reduce it by changing the economics of this significant illegal economy. In doing so, we will experience many benefits, including instilling trust in global interconnected systems, creating new jobs while reducing a skills shortage, and increasing the diversity of the workforce.

Thank you Chairman Thune, Ranking Member Nelson and distinguished Members of the Committee for the opportunity to provide IBM Security's perspective on this important topic.

The CHAIRMAN. Thank you, Mr. Barlow.
Mr. Ganesan?

**STATEMENT OF VENKY GANESAN, MANAGING PARTNER,
MENLO VENTURES; AND CHAIR, NATIONAL VENTURE
CAPITAL ASSOCIATION**

Mr. GANESAN. Thank you. Chairman Thune, Ranking Member Nelson, thank you for the opportunity to testify before the Committee this morning. My name is Venky Ganesan, and I serve as one of the managing partners of Menlo Ventures. We are one of the oldest and most successful venture capital firms in Silicon Valley.

We have been fortunate to be early investors in many iconic companies, including Gilead Sciences, Siri, and Uber. In the cybersecurity space, we were the lead investors in Q1 Labs, which is now a major part of IBM Security, and IronPort, which is a critical part of Cisco Security. I was one of the lead investors and on the Board of Palo Alto Networks, which today has a market capitalization of over \$10 billion. I am testifying today in my capacity as Chair of the National Venture Capital Association.

To understand the role that young high-growth startups play in emerging cybersecurity technology, it is important first to understand the role of venture capital in American entrepreneurship. Venture capitalists like myself invest in early stage companies with big potential and work shoulder-to-shoulder with entrepreneurs to build the company. If you think of a baseball team, the venture capitalist is a coach or manager, and the entrepreneurs are the players on the field. We are all working together to deliver value to the American public.

American entrepreneurship is the envy of the world, in significant part because of the right blend of public policy priorities, such as the tax code, that rewards long-term, patient investment of capital and Federal investment into basic research, which often forms the building blocks for new companies or industries.

Cybersecurity innovation and venture capital have been intertwined right from the beginning, as almost all of the major independent cybersecurity companies in the public market were funded by venture capitalists. I have great respect for all the companies and panelists here, but I'll tell you, most of the innovation in cybersecurity today happens at the early stage with startups.

Venture investors have deployed almost \$15 billion in more than 740 cybersecurity companies since 2010. These companies are pushing the outer boundaries of what is possible in cybersecurity.

We have the advent of many exciting new technologies that present incredible opportunities but also many challenges.

For example, artificial intelligence continues to be an area of considerable excitement among venture capital investors. It is undeniable that we have made significant progress in AI, even if a general purpose AI solution is not estimated to be available until 2045 or beyond. I encourage the Committee to think of AI applications not as man versus machine, but rather as man plus machine.

One of the biggest challenges in cybersecurity today is the avalanche of security alerts every enterprise gets. There's simply not enough security professionals in the world to resolve all of them. AI is a potential solution for this problem, because it can automate some mundane activities, thus freeing the experienced security professionals to focus their energies on the high-value alerts.

In my written testimony, I discuss other new cybersecurity technologies, such as blockchain, the Internet of Things, and quantum computing that offer further opportunities and risks. I believe this Committee can help spur cybersecurity innovation and protect Americans from future threats with policy action in a few areas, and I have a few recommendations.

First, we must modernize our procurement system so our government has access to world-class cybersecurity technology, much of which comes from startups. The unfortunate reality is our procurement practices act as a deterrent to many startups. If you look at the cybersecurity threats we face today, a lot of them were technologies that were created after 2014. So you need modern software technologies, and our procurement practices do not allow you to have access to that.

Second, the government can drive market solutions by establishing best practices. I commend Chairman Thune's efforts on the NIST Framework and recommend NIST develop a way to update the Framework periodically and establish test guidelines that all security products can be objectively compared against.

Third, we need a better legal framework that allows data sharing so that companies can team up against external threats, learn from each other, and benefit from each other's solutions.

Fourth, we should create a generation of cyber warriors, as attempts to weaponize technology will not recede in our lifetime. We have countries, like Israel, China, Russia, who all create a generation of cyber warriors that we've got to compete against. Our idea would be to set up a cyber academy where we can recruit, train, and develop the best young cyber talent in our country.

Fifth and finally, more must be done to facilitate cyber insurance to minimize existential risk, as the cost of breaches can be astronomical and beyond any single company's ability to handle. We need a market-based system to allow us to get feedback, and cyber insurance is a market-based system to do that.

To conclude, the cybersecurity challenges we face are daunting, but I'm an optimist. For 241 years, it has never made sense to bet against America, and that's not going to change. My personal investing experience gives me great confidence that there are many amazing companies out there who have needed solutions to our cybersecurity challenges. This Committee can support those dynamic young companies by enacting pro-entrepreneurship policies

that will facilitate creation of a new wave of cybersecurity innovation.

I look forward to your questions.

[The prepared statement of Mr. Ganesan follows:]

PREPARED STATEMENT OF VENKY GANESAN, MANAGING PARTNER, MENLO VENTURES
AND CHAIR, NATIONAL VENTURE CAPITAL ASSOCIATION

Chairman Thune, Ranking Member Nelson, thank you for the opportunity to testify before the Senate Committee on Commerce, Science, and Transportation today. My name is Venky Ganesan and I serve as one of the Managing Partners of Menlo Ventures. Menlo Ventures is one of the oldest (41 years) venture capital firms in Silicon Valley. We manage approximately \$4.5 billion in assets and have invested in over 400 portfolio companies whose aggregate value if held post going public would be over \$200 billion. We have been fortunate to be early investors in many iconic companies, including F5 Networks ("FFIV"), Gilead Sciences ("GILD"), Hotmail (acquired by Microsoft), Siri (acquired by Apple), and Uber. We also have a long and successful history investing in cybersecurity. Menlo Ventures was the lead investor in Q1 Labs, which was acquired by IBM and has now become a major part of IBM Security. Additionally, Menlo was also the lead investor in IronPort, which was acquired by Cisco for \$830 million and is a critical part of Cisco Security. I was one of the lead investors and was on the board of Palo Alto Networks ("PANW") which today has a market capitalization of over \$10 billion. I am here today in my capacity as Chair of the National Venture Capital Association (NVCA), which advocates for pro-entrepreneurship policies that create jobs and grow the U.S. economy.

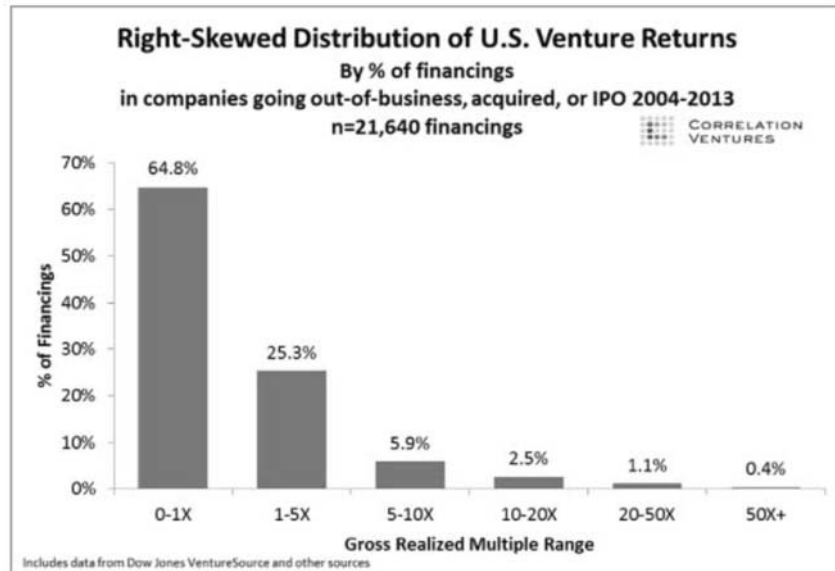
Venture Capital and Entrepreneurship

Venture capital and entrepreneurship go hand in hand. Some people mistake venture capital as a passive investing function in which venture capitalists pick companies, write checks, and then wait for the returns to roll in. While that would be nice, the reality is much different. A better analogy to understand the relationship between venture capitalists and entrepreneurs is to think about startups like a baseball team. The entrepreneurs are the players on the field. The venture capitalists are the coach and the managers. Ultimately, the players need to deliver on the field and that is what entrepreneurs do. However, as the coach/manager, venture capitalists help recruit players, negotiate contracts, run training sessions, make real-time tactical decisions during the game, and decide on the playing roster.

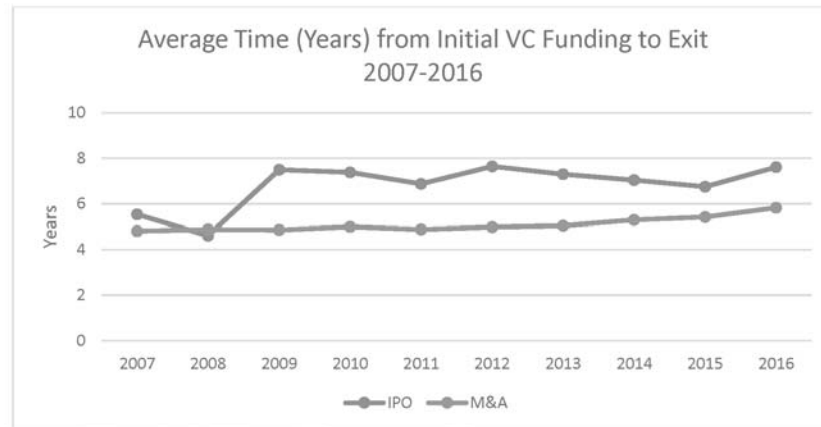
To give you additional context, in the last three weeks I have personally done the following:

- Evaluated over 5 new investments;
- Negotiated compensation agreements with a CEO;
- Identified and sourced potential executives for one of our companies;
- Interviewed and convinced a young marketing executive to join one of our companies;
- Done reference calls with prospective customers and encouraged them to buy from one of our early stage companies; and
- Held strategy sessions with salespeople from our portfolio companies.

Venture capital is hard and unfortunately not always successful. According to research by Professor Shikhar Ghosh of Harvard Business School, 75 percent of venture backed startups do not return investors capital. Correlation Ventures, which evaluated over 21,000 financings spanning the years 2004–2013, showed that 64.8 percent of financings resulted in less than 1x return of capital.



Even when venture capitalists are successful, it takes a long time. The average time to exit for venture-backed startups according to the NVCA 2017 Yearbook is more than 5 years for an acquisition and more than 7 years for an initial public offering (IPO). In life science, those time periods are often even longer.



Source: NVCA 2017 Yearbook, Data Provided by PitchBook

However, when venture capital works, it really works. Some of the most prominent technology companies in the world, *e.g.*, Facebook, Twitter, Snapchat, Google, Amazon, Microsoft, etc., were all venture backed. At one point in 2016, the five largest companies by market capitalization in America were technology companies (Apple, Microsoft, Alphabet, Amazon, and Facebook) all of whom were venture-backed. Three of these companies were built with venture capital within the last 22 years. According to a 2015 study by Ilya Strebulaev of Stanford University and Will Gornall of the University of British Columbia, 42 percent of all U.S. company

IPOs since 1974 were venture-backed.¹ Collectively, those venture-backed companies have invested \$115 billion in research and development (R&D), and created \$4.3 trillion in market capitalization, accounting for 85 percent of all R&D spending and 63 percent of the total market capitalization of public companies formed since 1974. Specific to the impact on the American workforce, a 2010 study from the Kauffman Foundation found that young startups, many of them venture-backed, were responsible for almost all the 25 million net jobs created since 1977.²

These incredible contributions to the U.S. economy are due, in significant part, to the right blend of public policy priorities. For example, our tax code rewards long-term, patient investment of capital that enables venture capitalists to work alongside entrepreneurs for many years before they see any return on investment. I encourage all Members of Congress to make new company formation a priority in tax reform. In addition, the Federal Government has prioritized investment into basic research, which often forms the building blocks for new companies and even whole industries that fuel economic growth with rapid advancements that improve our well-being and extend our lives.

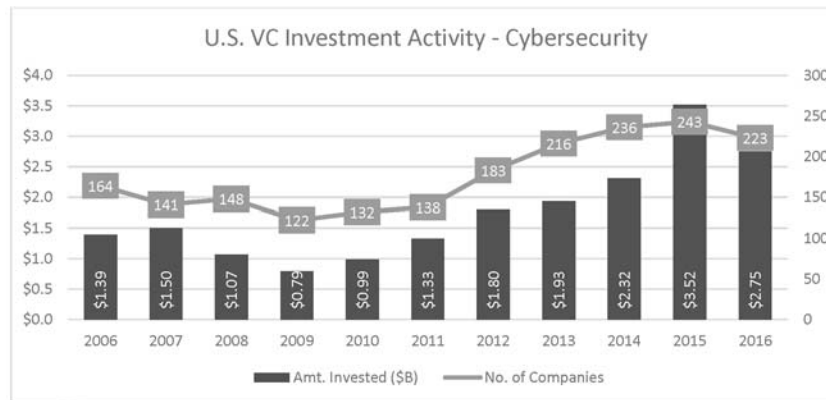
Venture Capital's Impact on Cybersecurity

Cybersecurity innovation and venture capital have been inextricably intertwined right from the beginning. Some of the biggest innovations in cybersecurity have been introduced by venture capital backed startups. For example:

- The stateful inspection firewall which is a critical component of almost all perimeter security products was invented by Checkpoint;
- SSL encryption was invented by Netscape; and
- Next generation firewall based on a “single pass” architecture was pioneered by Palo Alto Networks.

In addition, almost all of the major independent cybersecurity companies in the public market were funded by venture capitalists, including Symantec, Palo Alto Networks, FireEye, Proofpoint, Imperva, Fortinet, Qualys, and Cyberark, to name a few.

Venture capitalists are also incredibly active in the private markets. Since 2010, they have invested over \$14.6 billion in more than 740 cybersecurity companies including \$3.52 billion in 2015 and \$2.75 billion in 2016.³



Source: PitchBook-NVCA data

America's leadership in cybersecurity is directly attributable to the strong expertise and significant patient investment capital provided by U.S. venture capitalists.

¹ "The Economic Impact of Venture Capital: Evidence from Public Companies," Stanford University Graduate School of Business Research Paper No. 15-55, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2681841.

² "The Importance of Startups in Job Creation and Job Destruction," Kauffman Foundation Research Series: Firm Foundation and Economic Growth," (July 2010), available at http://www.kauffman.org/~media/kauffman.org/research%20reports%20and%20covers/2010/07/firm_formation_importance_of_startups.pdf.

³ Pitchbook-NVCA data (Note: Some companies raised a round of venture funding in more than one year, in which case they are counted separately in each year.)

Cybersecurity Threat Landscape

Cyber threats at a consumer level really started to emerge in the 1990s with the commercialization of the Internet. Until the advent of the Internet, viruses could only pass to other computers through floppy disks or other storage media. Once consumers and businesses started connecting their computers to the Internet, viruses with names like Melissa and ILOVEYOU could propagate massively across the Internet and infect millions of users. The first generation of protection against these viruses were anti-virus companies such as Symantec and McAfee that used signature based techniques to create anti-virus software. In order to protect themselves from hackers, corporations started implementing perimeter security solutions. Prominent among these solutions were firewalls, Intrusion Prevention Systems (IPS), and Intrusion Detection Systems (IDS). While there was a cat-and-mouse element to this fight, for the most part people felt that the cybersecurity problem was in check until the advent of two major developments.

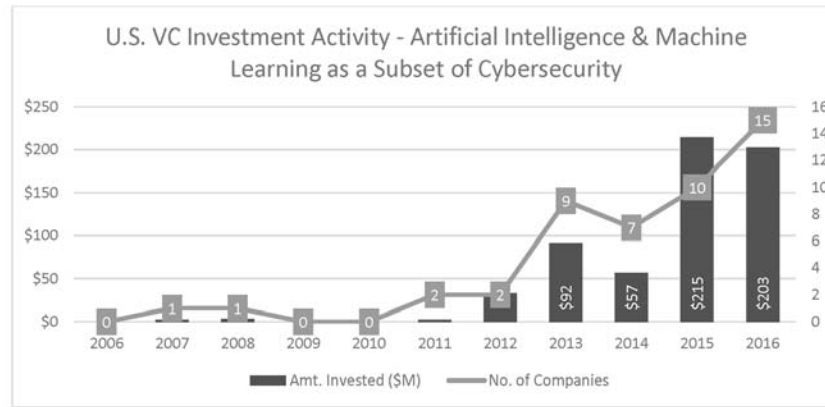
- The first major development was a discovery by researchers in 2010 of a malicious computer worm known as Stuxnet that targeted industrial computer systems. What made Stuxnet different from other viruses was that it targeted programmable logic controllers (PLC) which were not connected to the Internet and were previously thought to be unhackable. Stuxnet showed that many elements of our critical infrastructure, such as dams, electric grids, water treatment facilities, hospital systems, factory assembly lines, and power plants, which use supervisory control and data acquisition (SCADA) and PLC systems, are now under threat, even when they are not connected to the Internet.
- The second major development was the advent of highly sophisticated malware called Advanced Persistent Threats (APT) in 2013. These malwares function quite differently from the viruses of the past. The hackers goal is espionage and data theft. Once they infect a target, they use sophisticated root kit techniques to disguise themselves. They then connect to command and control servers on the Internet and both exfiltrate data and take new instructions. These sophisticated malwares can remain undetected for months or even years while slowly traversing across the entire network of the victim and grabbing valuable data. All the big breaches you have heard about recently—Anthem, Office of Personnel Management (OPM), Target, Sony—were victims of this technique. Legacy security vendors never architected their solutions to handle threats like this, and unless governments, enterprises, and consumers upgrade their security infrastructure to a modern architecture they are all exposed to this threat.

In addition to these new threats, there are some major developments in other technical areas such as artificial intelligence, Blockchain, Internet of Things and quantum computing which have the potential to impact cybersecurity. Below is a brief overview of each of these emerging areas of technology and how they might impact cybersecurity.

Artificial Intelligence/Machine Learning

Artificial intelligence (AI) in a computer science context is defined as the study of intelligent agents. It is the idea that computers mimic cognitive functions such as “learning” and “problem solving” that is normally associated only with humans. Prominent milestones in AI include IBM’s Deep Blue becoming the first computer chess-playing system to beat a reigning world champion, IBM’s Watson defeating two Jeopardy champions, and Google’s AlphaGo beating a professional Go champion. In popular culture, AI is usually captured as the evil machines taking over the world a la “Hal” in the movie “2001: A Space Odyssey” or “The Matrix.”

Artificial intelligence and machine learning have been areas of considerable excitement among venture capital investors. As a subset of U.S. cybersecurity venture investment, 15 artificial intelligence and machine learning companies raised \$203 million in 2016. In 2015 and 2016, 21 companies raised a combined \$417 million in venture funding. To put this into context, only 13 companies raised a total of \$191 million from 2006 to 2014.



Source: PitchBook-NVCA data (Note: Some companies raised a round of venture funding in more than one year, in which case they are counted separately in each year).

It is undeniable that we have made significant progress in AI. The factors that have enabled this progress include the availability of inexpensive computing through the cloud through such innovation as Amazon Web Service (AWS), sophisticated machine learning techniques and algorithms, and availability of huge data sets to be used as training data. Some of the progress we have made towards a self-driving car is directly attributable to machine learning techniques like “Deep Reinforcement Learning.” To date, artificial intelligence and machine learning seems to show strong results when we apply it to a narrow problem or constrain the solution space, *i.e.*, Chess, Go. However, we are not close to a general-purpose AI solution any time soon. While estimates vary considerably, no credible expert estimates that we will have general purpose AI sooner than 2045.

Rather than thinking in the context of Man vs. Machine, a better exercise would be to think in the context of Man *plus* Machine. But, as we come to rely on this technology to bolster our capabilities, could hackers and nation state actors use artificial intelligence to hack into our cyber infrastructure? Here again the answer is mixed. We are far from an AI machine that can hack any infrastructure in a general-purpose way. However, people could use machine learning techniques to make progress. Still, most experts believe that the existing techniques of capitalizing on human error (*e.g.*, clicking on malware links, opening attachments) are so effective that there currently is little incentive to invest in expensive AI research for cyber hacking. On the positive side, there are a variety of startups trying to use AI/machine learning to help automate security operations. One of the biggest challenges in cybersecurity today is the avalanche of security alerts every enterprise gets. There are not enough security professionals in the world to chase down and resolve every security alert. There has been some promising advances in using artificial intelligence to automate some of these mundane activities thus freeing the experienced security professionals to focus their energies on the high value alerts.

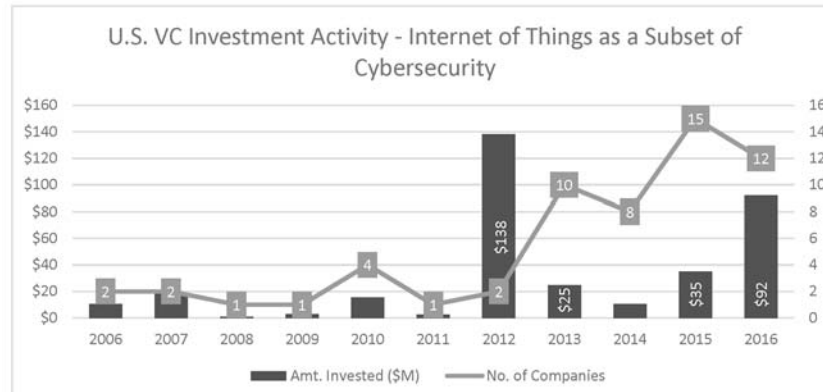
Internet of Things (IoT)

The Internet of Things refers to the inter-networking of physical devices, vehicles, connected devices, and buildings whereby physical objects can collect and exchange data with each other. The canonical example of IoT are smart TVs, which are connected to the Internet and allow you to watch over-the-top content not available through your cable or satellite feed. Another example would be a connected car, such as a Tesla, which can be upgraded or modified with an over-the-air software update.

IoT interfaces with cybersecurity in two major ways. First, as more and more appliances get “connected” and join the Internet they are now vulnerable to hacking. Recent reports have shown that state actors and sophisticated hackers can take over connected devices such as TVs, refrigerators, vehicles, and yes, even microwaves. Once taken over, these devices can then be used to spy and gather confidential information. A good example of this would be voice assistants like Amazon Echo and Google Home. These devices are connected to the Internet and are always listening for voice commands. A hacker could take over one of these devices and listen and record all voice conversations happening around the device.

Second, and even more worrying, is that these devices once taken over can be used as a weapon in a broader attack. There was a major denial of service attack (DDOS) in October 2016 targeting a domain name service (DNS) provider called Dyn. This attack brought down Dyn, which in turn affected major parts of the Internet, including major websites such as Amazon, Airbnb, Comcast, and The New York Times. It was discovered that the attack was orchestrated through a botnet consisting of millions of IoT-enabled devices, such as webcams and cameras. An additional concern would be the ability of hackers to take over the controls of a connected car and use it as a weapon for terrorism purposes. The structure of the consumer electronics industry perpetuates and exacerbates these security threats. Consumers are not well informed about the inherent security risks in these products to demand strong security solutions and there are not well-established security certifications for consumer devices. As a result, vendors often have not made the necessary investments in product security, and have not implemented even basic capabilities such as password management or the ability to perform over-the-air security upgrades.

In 2016, 12 cybersecurity IoT companies raised \$92 million in venture funding, the second highest annual total for both metrics in the past decade.



Source: PitchBook-NVCA data (note: some companies raised a round of venture funding in more than one year, in which case they are counted separately in each year).

Blockchain

Blockchain refers to a digital ledger in which transactions made in Bitcoin or any other cryptocurrency are recorded chronologically and publicly. Blockchains are critical for the functioning of cryptocurrency since they act as the ledger of record to show who owns what and how ownership changes from one person to the other. Regardless of your views on cryptocurrencies, experts are excited about Blockchain because it is a distributed database with built in validation. Blockchain is effectively an independent, transparent, and permanent database existing in multiple locations and shared by a community. No person controls it, nor can anyone manipulate it so it can serve as the single source of truth for transactions. Blockchain can be used to document anything, including record titles of digital goods.

Blockchains are exciting from a cybersecurity perspective since they are currently perceived as much safer than traditional databases and less impervious to manipulation and fraud. The drawback of Blockchain, however, is that as they scale and get big, they need massive computational power, which in turn needs significant electrical power. Recently, a financial institution estimated that if 400 different virtual currencies were created, they would need 200 times the amount of electrical power Ireland consumes. Governments who have access to unlimited computational and power resources should however consider Blockchain as a promising way to store their critical data. High-profile hacks of databases like with OPM demonstrate the vulnerability of information held by the government. Blockchain could play an important role in data authentication and transparency in the healthcare and financial sectors. There are numerous use cases through which Blockchain could be used for identity and key management, domain name system (DNS) authentication, and patient record management.

Quantum Computing

Traditional computers encode their data in binary form, *i.e.*, data is stored either as a 0 or a 1. There are only two states and traditional machines read these binary files, which are just sequences of 0s and 1s and make sense of them. Quantum computers, on the other hand, store their data in something called “qubits”. A quantum computer with n qubits can store a complex combination of up to 2^n states. The technical details are quite complex and complicated to explain, but a simplistic way of thinking about it is that a quantum computer will allow you to solve certain computer problems that are intractable on conventional computers.

The way quantum computing intersects with cybersecurity is that all of our current encryption standards are based on traditional computing standards. If a large-scale quantum computer can be built, then our current public key cryptography standards (*e.g.*, RSA, ECDSA, DSA) could all be broken, allowing anyone to decrypt the data. The best estimates for what it takes to build such a quantum computer, according to National Institutes of Standards and Technology (NIST), are 15 years, \$1 billion in spend, and electrical power tantamount to a small nuclear power plant. This is beyond any private actor, but possible for a state actor like China or Russia who do have the resources to invest in quantum computing. This is a possibility that should greatly concern policymakers because if we are beaten in this race the country could be at a severe strategic disadvantage. Fortunately, we do have a number of academics developing post-quantum cryptography. There is reasonable confidence that we can find acceptable cryptographic techniques capable of withstanding quantum computing attacks in the future. My view is that quantum computing is still very nascent and not close to commercialization. There are far more immediate acute problems in cybersecurity that demand action before we need to focus on quantum computing.

Recommendations

As an experienced investor in cybersecurity and a concerned citizen of this great country, I have a few recommendations for the Committee to consider on this topic:

1. *Modernize government procurement systems so that the government has access to the best technologies:* The world’s best cybersecurity solutions are developed in America but unfortunately our government’s procurement laws are outdated and make it hard for young startups to sell to the government. As noted before, sophisticated malware threats like APT can only be countered by modern security software. I do want to acknowledge the efforts of entities such as In-Q-Tel⁴ and DIUx⁵ that have made progress in helping startups interface with government. However, these initiatives are focused on the defense side of the government and do not help any of the Federal agencies focused on civilian issues. Our procurement practices are based on old frameworks that view software solutions in a static, object-oriented way. The fact is, modern software is cloud based and updated continuously and our procurement practices need to evolve to accommodate that. As a starting point, the Committee should collaborate with agencies within its jurisdiction to improve their procurement practices to better enable purchase of startup-generated technology. Beyond that, I recommend a more comprehensive examination of Federal procurement practices by the Trump Administration to ensure the best technology is used to defend our government against 21st century threats.
2. *Setting standards around cyber-hygiene:* One way the government can help drive market solutions is by setting standards around cyber hygiene and expectations. I do want to commend this Committee’s leadership and support, especially Chairman Thune’s efforts in regard to the Cybersecurity Framework proposed by NIST. I recommend that NIST develop a systematic way to update the Cybersecurity Framework periodically and also establish test guidelines that all security products can be objectively compared against. In cybersecurity, we are only as strong as our weakest link so it is imperative that we create incentives for industry participants to practice cyberhygiene. I would caution,

⁴ In-Q-Tel is “is the non-profit strategic investor that accelerates the development and delivery of cutting-edge technologies to U.S. Government agencies that keep our Nation safe.” See <https://www.iqt.org/>. In-Q-Tel is a member of NVCA.

⁵ With locations in Silicon Valley and Boston, “Defense Innovation Unit Experimental (DIUx) serves as a bridge between those in the U.S. military executing on some of our Nation’s toughest security challenges and companies operating at the cutting edge of technology . . . [DIUx] continuously iterate[s] on how best to identify, contract, and prototype novel innovations through sources traditionally not available to the Department of Defense, with the ultimate goal of accelerating technology into the hands of the men and women in uniform.” See <https://www.diu.mil/>.

however, that whatever solutions that may be crafted in this area be limited in scope and remind lawmakers to be careful not to unduly interfere in business practices which can lead to unintended consequences.

3. *Enable legal frameworks for companies to share and exchange data:* There is limited information flow today between companies and government. The CIA and NSA possess very sophisticated techniques and detailed information about threats and malwares, but there is no systematic and safe way for that expertise to be shared with the civilian sector. There is also minimal data sharing between companies, as people are worried about legal liabilities from disclosing data around breaches and malware. We need a better legal framework that allows more data sharing so that companies can team up against external threats, learn from each other, and benefit from each other's solutions.
4. *Create a generation of cyberwarriors:* Countries like Israel have sophisticated programs like Talpiot that identify talented high schoolers in computer science and orient them to cybersecurity careers. We need to create a generation of cyberwarriors and should consider different strategies, including perhaps setting up a cyber-academy like the U.S. Naval Academy where we can recruit, train, and develop the best young cyber talent in our country. Attempts to weaponize technology will not recede in our lifetime; it is time for us to build our institutions to recognize this fact.
5. *Use cyberinsurance to pool and minimize existential risk:* Regardless of how much precaution companies take, there is always a risk of security and data breaches. The cost of these breaches can be astronomical and beyond any single company's ability to handle. Similar to earthquakes and hurricanes, we need to develop a deep cyberinsurance industry so that companies have a way to pool and minimize existential risk.

Conclusion

The challenges we face in cybersecurity are daunting, but I am an optimist. The pilgrims on the Mayflower faced insurmountable odds but found a way to build a home and a country that is the leader of the free world. My own personal investing experience gives me confidence that there are market-based approaches that can be used to battle the cybersecurity conundrum.

In 2011, two MIT graduate students applied for a small grant from the National Science Foundation (NSF) with an idea to create a cybersecurity ratings organization. In 2013, Menlo Ventures, along with other venture firms, funded them. Six years later, their company—BitSight Technologies—employs 225 people, counts more than 700 customers across 25 different sectors, and has raised \$95 million in venture funding. The company was recently named a Forbes “Next Billion Dollar Startup.”

As a cybersecurity ratings company, BitSight measures the security performance of organizations on a scale of 250–900. A higher rating indicates better security performance. It is a simple concept—very similar to the credit ratings model companies such as Moody's and Standard & Poor's have championed for credit and debt.

BitSight is an example of a venture-backed cybersecurity company providing market-based solutions through its ratings system. It is a system that can be used by market participants that can quantitatively improve the global state of cybersecurity. BitSight is also an outstanding example of how government and the private sector can work together to solve our cybersecurity challenges. What started as an NSF grant turned into a successful company that was backed by private, risk capital. Our firm's long-term investment is rewarded because policymakers understand the value of that investment to our national economy. Due to this collaboration, American jobs were created and cybersecurity challenges are being addressed. If we all continue to work together, we can achieve a tremendous amount.

Finally, my greatest recommendation is to use all policy tools available, including tax and regulatory policy, immigration, patent, and Federal investment in basic research, to encourage new company formation. It is through the innovation created by entrepreneurs partnering with venture capitalists that we will have the greatest chance to defeat this challenge.

The CHAIRMAN. Thank you, Mr. Ganesan.
Mr. Grobman?

**STATEMENT OF STEVE GROBMAN, INTEL FELLOW AND CHIEF
TECHNOLOGY OFFICER, INTEL SECURITY GROUP**

Mr. GROBMAN. Good morning, Chairman Thune, Ranking Member Nelson, and members of the Committee. Thank you for the opportunity to testify today. I'm Steve Grobman, Intel Fellow and Chief Technology Officer for the Intel Security Group.

I've been focused on cybersecurity technology for the good part of over two decades. With every advancement in technology, it introduces new challenges. When we introduced automotive and commercial air transport in the 20th century, it radically changed every element of American life. But it also introduced new challenges we needed to think about related to safety and security.

The technologies we're going to speak about today are quite similar. We're going to focus on IoT. With Moore's Law and enhanced connectivity, 50 billion connected devices will be in the marketplace by 2020, according to IDC. This drives new risk, not only in manufacturing and critical infrastructure, but also in connected consumer devices.

Last October, we saw the weaponization of consumer devices all over the world that were used not to attack the consumers themselves, but rather to be turned into a weapon and targeted against some of our tech providers, such as Twitter, Spotify, and others. This is a large part of the challenge in securing these consumer devices, in that market forces don't naturally drive manufacturers to build secure architectures or maintain those devices throughout their useful life.

We'll also have the opportunity to talk today about artificial intelligence. Artificial intelligence powers everything from our future self-driving cars to search engines. The underlying technologies are powerful tools for both cyber attackers as well as cyber defenders. Attackers are using these technologies to do everything, such as optimize spear-phishing, to better select the targets that they will go after, while defenders are using this technology to better classify malware, to identify the threats that are in their environment, and to fundamentally process the massive quantities of data that exist in their organization.

We must always be mindful that as new defensive technologies are created to defend environments, bad actors will work to create countermeasures and evasion tactics to make these technologies less capable, and we must focus on that and be realistic, not only about the capabilities of technology but also the limits, as we look to benefit from them.

We'll be talking today about blockchain. Blockchain creates algorithms which solve major problems associated with transactions, identity, supply chain, and other fields, using a highly-resilient ledger capability that prevents you from having to rely on a trusted middleman. Unfortunately, this also powers some of the tools that bad actors use to facilitate some of the most challenging cyber crimes that we see today, including things like ransomware, where the ability to have anonymous transactions allow cyber criminals to get paid directly from the victims. So we must recognize how these new innovations will not only be used to add efficiencies and solve large challenges, but how they will become valuable tools for the attacking community.

We will have the opportunity to talk about quantum computing. Quantum computing is an amazing innovation to solve some of the most challenging research problems we're facing. But quantum computing is also well suited to attack some of the encryption protocols and algorithms that we rely on today. Things like the RSA public key algorithm is subject to future quantum attacks. There are other algorithms that are not subject to quantum attacks. We call these quantum safe, things like the AES algorithm that we use for bulk encryption. These algorithms are used pervasively together to secure the way we communicate and store data.

What we must recognize is that this is not a problem to worry about only in the future, but today, because bad actors, nation states can put data on the shelf today, and as these encryption capabilities are broken in the future, they will be able to access that data. So we must recognize how to identify new algorithms that are quantum safe today as well as triage the systems that rely on protecting data so we protect data in its greatest form.

We'll be talking about making specific recommendations on regulations. We will be talking about not wanting to rely on hard regulations, in that cyber crime evolves very quickly, meaning that what the threats are today will not be the threats of tomorrow, and being overly prescriptive into what a manufacturer or organization might do will create opportunity costs that are better spent on protecting their environment.

We also need to be more transparent in our vulnerabilities equities process, where we need to recognize government will identify or have access to vulnerabilities, and we need greater transparency in how we disposition those.

I thank you very much for the opportunity to talk today, and I look forward to our discussion.

[The prepared statement of Mr. Grobman follows:]

PREPARED STATEMENT OF STEVEN GROBMAN, INTEL FELLOW AND CHIEF
TECHNOLOGY OFFICER, INTEL SECURITY GROUP

Good morning, Chairman Thune, Ranking Member Nelson, and members of the Committee. Thank you for the opportunity to testify today. I am Steve Grobman, Intel Fellow and Chief Technology Officer, Intel Security Group, part of Intel Corporation.

I am pleased to address the Committee on how emerging fields like Artificial Intelligence (AI), Internet of Things (IoT), quantum computing, and Blockchain not only create tremendous value for American citizens, but also present new opportunities for both attackers and defenders in the field of cybersecurity. My testimony will address Intel and Intel Security's commitment to cybersecurity and the state of the above emerging technologies. I will conclude with some policy recommendations.

First, I would like to provide some background on my experience and Intel's commitment to cybersecurity. I am the Intel Security Group Chief Technology Officer (CTO), responsible for leading technical innovation and thought leadership related to cybersecurity at Intel. I have been focused on the field of cybersecurity for over two decades in a wide range of positions.

Intel Security's Commitment to Cybersecurity

Intel is a global leader in computing innovation, designing and building the essential foundational technologies that support the world's computing devices. Combining Intel's decades-long computing design and manufacturing experience with Intel Security's market-leading cybersecurity solutions, Intel Security brings a unique understanding of the cybersecurity challenges threatening our Nation's digital infrastructure and global e-commerce. Governments, businesses and consumers face a cybersecurity threat landscape that is constantly evolving with each new technology that is brought to market at a faster pace than ever before. The sharp

rise of internet-enabled devices (known as “Internet of Things” or “IoT”) in government, industry and the home exacerbates this already difficult challenge. The increasing advancement of artificial intelligence provides real promise for society but at the same time provides a tool for malicious actors as well. Emerging areas such as quantum computing have repercussions we need to be addressing now, and blockchain is a strong technology that can be used to solve fundamental problems in security such as trusting a central authority. The challenges we face are too significant for one company or entity to address on its own. Real change in cybersecurity requires a true public-private partnership with industry.

Collaboration will be the driving force behind what soon will be the new McAfee (currently known as Intel Security)—planned to be a standalone company this year. It’s also why we recently announced a whole new ecosystem of integrated platforms, automated workflows and orchestrated systems based on an open communications fabric that will enable all of us in cybersecurity to work together in ways never before thought possible.

Emerging Technological Areas of Value and Concern

With every advancement in technology, new challenges are introduced. The mass adoption of automobiles and air travel fundamentally transformed every element of life in the 20th century, yet these innovations also caused us to look at new concerns and challenges related to auto and air safety. The technologies we will discuss today are very similar. Technologies related to the Internet of Things, artificial intelligence, quantum computing and blockchain are foundational technologies with the potential to improve health, cure disease and add new levels of automation and efficiency to our economy and everyday life. These same building blocks will be valuable tools to both offensive and defensive participants in the cybersecurity domain. This discussion will focus on how these capabilities are pivotal to building new security defensive architectures, but also examine what we need to recognize related to new threats and risks the technologies facilitate.

Internet of Things (IoT)

The combination of Moore’s law¹ and pervasive connectivity have lowered the barrier of entry in building and enabling “smart and connected” devices in almost every aspect of business and consumer life in America. Collectively we are referring to these devices as the “Internet of Things,” or IoT.

IoT is defined as endpoint devices such as cars, machinery or household appliances that connect to the Internet and generate data that can be analyzed to extract valuable information. There are three sub-definitions emerging out of the IoT space; however, all three definitions overlap. The “Mobile IoT” comprises devices like cars, wearables, sensors and mobile phones, which all connect directly through broadband wireless networks. The “Industrial IoT” connects devices in industrial environments like factory equipment, security cameras, medical devices and digital signs. These devices are able to connect to the Internet and into the datacenter (cloud) through an industrial “gateway.”² Finally, the “Home IoT” connects devices like game consoles, smart TVs, home security systems, household appliances and thermostats through a gateway to the internet.

IoT presents staggering economic opportunities for the U.S. and the world. Market research firm IDC estimates there will be 50 billion connected devices in the marketplace by 2020³, and Morgan Stanley forecasts 75 billion in that same time period.⁴ These estimates would equate to six to 10 connected devices for every person on earth. Whether the exact number of devices is 50 billion, 75 billion or something more, one thing is for certain: The number of connected devices will explode in the next five years. In just the automotive industry alone, it is projected that 250 million (or one in five) cars worldwide will be connected to the Internet by 2020—via

¹ In 1965, Gordon Moore, one of Intel’s co-founders, made a prediction that would set the pace for our modern digital revolution. From careful observation of an emerging trend, Moore extrapolated that computing would dramatically increase in power, and decrease in relative cost, at an exponential pace—from 50 Years of Moore’s Law Intel article—<http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html>

² A gateway is a node on a network that serves as an entrance to another network.

³ Business Strategy: The Coming of Age of the “Internet of Things” in Government, IDC (April 2013), <http://www.idc.com/getdoc.jsp?containerId=GIGM01V>

⁴ Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020, Business Insider (Oct. 2 2013) <http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10>

technologies like LTE, satellite and 5G communications networks.⁵ To put this in perspective, there were roughly 250 million cars on U.S. roads in 2013.⁶

This explosion of devices and technological revolution that is IoT is projected to have a staggering positive impact on the U.S. and global economy. McKinsey projects IoT will have a \$2.7 trillion to \$6.2 trillion global economic impact by 2025.⁷ And what should most excite U.S. policymakers is that the U.S. and other developed economies are expected to capture a remarkable 70 percent of this economic impact, if we develop a leadership position.

On the other hand, with the growth of IoT, we are rapidly approaching 50 billion connected devices (with varying degrees of security) that are becoming more and more valuable to attackers. We have already seen the beginnings of this trend, as cyberattacks against physical assets—from cars to electric power stations—move from science fiction to reality.

It is critical to recognize why IoT devices are interesting targets for a cyber attacker. Incentives may range from a cybercriminal monetizing an attack by holding a manufacturing facility for ransom or a terrorist or nation-state actor executing an attack on critical infrastructure or business assets to harm the U.S. economy or cause loss of life. As we will see, a key incentive for the bad actor may be to expand the attack infrastructure and weaponry they have at their disposal.

One of the major issues in consumer IoT is weak market incentives to drive manufacturers to build strong architectures, as the consumer buying the device currently places little value on security, especially with tight margins in the consumer IoT industries. More worrisome is that manufacturers generally don't maintain the security of a device throughout its entire practical life. Although a smart TV or thermostat may have a three-year warranty, the device will likely function for many years beyond that. If security vulnerabilities are identified in year five, is the manufacturer compelled to release a fix? What about manufacturers that no longer exist? With the rate and pace of the creation of smart and connected devices, it is inevitable there will be millions of vulnerable orphaned devices that will be ripe for exploitation.

One thing critical to understand is that this is not just a consumer problem. One of the questions I'm often asked is why someone should care if their light bulb is hacked. What data are they really going to steal? And the thing is, they're not going to steal data. That's not the concern. The concern is weaponizing that lightbulb to become part of the larger attack scenario. And that attack scenario can impact infrastructure, it can impact organizations and it can impact companies. The impact of insecure consumer devices is an issue that needs to be comprehended well beyond just the consumer who purchased the device.

This is exactly what we saw in October 2016 with the Mirai attack. You may also hear it called the Dyn attack because it was targeting the Dyn DNS infrastructure. Mirai was a botnet that spread by finding generally inexpensive internet-connected consumer devices. These devices didn't have traditional vulnerabilities; they were vulnerable because the manufacturers had left integrated privileged accounts with weak passwords. The botnet grew by having compromised devices play two roles. They would search for other vulnerable devices and "recruit" them to join the botnet as well as check in with a command and control infrastructure to see if there were any attack actions they needed to take. The attackers who launched this attack issued a set of commands that flooded the Dyn infrastructure, resulting in major technology sites falling off-line for the better part of a day. The attackers could use this infrastructure to attack any organization, and we should think of the October incident as merely the beginning of this type of scenario.

To prove this out, my team ran a test in January, months after this attack. The experiment consisted of placing a simulated vulnerable device on an open network to see how long it would take a device to get compromised by this botnet. Literally at the one minute, six second mark, it was exploited. If this were a real device it would now be part of the broader botnet infrastructure.

When we think about attack scenarios it comes down to understanding one thing—risk. Security upgradability and patching are critical. Vendors need to design

⁵Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities, Gartner Inc. (Jan. 26, 2015), <http://www.gartner.com/newsroom/id/2970017>.

⁶Average Age of Vehicles on the Road Remains Steady at 11.4 years, According to IHS Automotive, IHS (June 2014) (253M cars on U.S. roads in 2013), <http://news.ihsmarket.com/press-release/automotive/average-age-vehicles-road-remains-steady-114-years-according-ihs-automotive>.

⁷Disruptive Technologies: Advances that will transform life, business, and the global economy, McKinsey Global Institute (May 2013), http://www.mckinsey.com/insights/business_technology/disruptive_technologies.

these critical capabilities into the products they offer to consumers. They also need a plan to deal with critical security vulnerabilities discovered even after devices are out of warranty. We also need to raise consumer awareness so that buying decisions have people consider security the way they think about other things today (*e.g.*, is this device from a reputable manufacturer? How long will it last?, What is the warranty?).

There are a number of technologies and approaches to device initiation and onboarding that Intel, its partners and customers are working on. We look forward to working with organizations like NIST to standardize where appropriate. However, the issue of legacy devices is more difficult to resolve, especially since it is likely in the hands of consumers to address.

Artificial Intelligence

Artificial intelligence (AI) comprises a broad field of technology that is enabling everything from our search engines to future self-driving cars and everything in between. It is important to think of AI as a set of technologies as opposed to one thing. Just as with every other technology in computer science, the attacker and defender communities analyze how AI can be used to enhance the capabilities of their solutions.

Attackers are using capabilities in AI to perform a wide range of tasks. AI can be used to automate capabilities that formerly required human analysis for high levels of effectiveness. For example, in spear-phishing the attacker's objective is to craft a message that the victim will trust or interact with. AI also can be used to build customized content automatically for a specific user based on content found within their social media information or other feeds. This customized content has a much higher success rate than a generic phishing interaction that is not user specific. Additionally, in the past the attacker had to choose between sending a high-volume of low-quality phishing interactions or a low volume of high-quality interactions that were crafted by a human. AI allows the attacker to have the best of both—a high quality phishing interaction that can be sent to a large number of users.

Another area where AI is an asset to cyber attackers is in victim selection. One capability AI is very well suited for is classification and scoring based on input data. One use case would be determining which of a set of potential targets or environments would be viable to breach. Attackers can train their data based on attributes about their environments and the effectiveness of past attacks and then focus their efforts where they will attain the highest return on their efforts and investment.

By the same token, the characteristics of AI make it a powerful tool in defensive tools and technologies for the cybersecurity industry. A large portion of a defender's job is processing massive quantities of data within an organization and identifying threats. There are also many elements in cybersecurity that are ultimately classification problems: Is a file malicious? Is behavior malicious? Is a user acting differently than the tasks they normally perform? All of these questions require data inputs, analysis and a predictive conclusion. AI has numerous classification capabilities and algorithms that make it a perfect tool for these sorts of tasks. For example, Intel Security has recently launched products such as our RealProtect technology⁸ that can analyze both the structure and behavior of an application using AI techniques to classify it as malicious or benign.

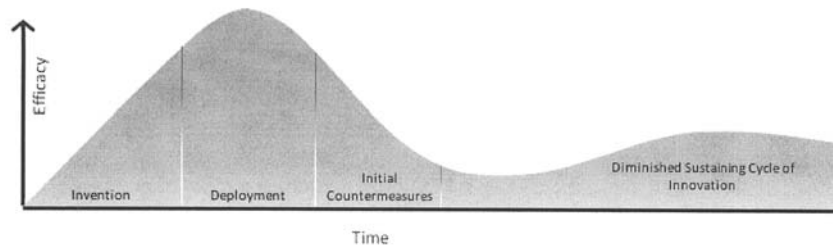
We do need to be mindful that our current state of the art in AI and analytics capabilities have limits, both in the field of cybersecurity as well as in other fields. Simply having massive quantities of data does not necessarily mean there is an underlying signal that can be teased out by an algorithm. We have radically improved how we do analytics on hurricane forecasting. For example, three days before a hurricane makes landfall we can predict where it will land to roughly 100 miles of accuracy, whereas 25 years ago, we could predict accuracy only to 350 miles.⁹ Yet, although we have massive quantities of seismic data, we have not yet found a way to reliably predict that a major earthquake is about to occur. The same issue occurs in cybersecurity; sometimes there is not a way to detect a threat based on the data available.

There is one element of AI in cybersecurity that separates it significantly from AI in other fields. In cybersecurity, there is a human bad actor who creates evasion tactics and countermeasures with the intent to have the algorithm fail. We don't have this issue in other forms of goal-based analytics (*e.g.*, water doesn't choose to change the way it evaporates as we get better at hurricane forecasting).

⁸ <https://www.mcafee.com/us/resources/white-papers/wp-real-protect-dynamic-application-containment.pdf>

⁹ https://en.wikipedia.org/wiki/The_Signal_and_the_Noise

In addition, in cybersecurity we see a trend where every new defensive technology loses effectiveness once deployment in the market drives adversaries to build countermeasures and evasion tactics. The cycle looks like this:



As we are on the leading edge of the deployment curve with many of the industry AI-based solutions, it is critical to use forethought into how bad actors will work to circumvent AI-based capabilities. Examples of techniques we are analyzing and tracking include machine learning poisoning and forcing defenders to recalibrate models or raise the noise floor. In the field of cybersecurity defense there is never a silver bullet defense, but rather a constant pipeline of innovation for both the attacker and defender.

Blockchain

Blockchains have gained a lot of attention as they provide key benefits across a wide range of applications. Blockchains first emerged as the technology behind the cryptocurrency Bitcoin. Blockchains, however, have much broader use cases, including identity management, marketplaces and supply chain management. The potential of the technology is considered disruptive and has been described as potentially impacting transactions in the same way the Internet affected communications.

Blockchain makes use of cryptographically supported immutable ledger and distributed consensus protocols to facilitate the exchange of assets between two untrusted parties, eliminating the need for intermediaries. Any networked ecosystem with a central authority for transaction authorization could potentially use a blockchain in the future as a replacement. In more detail, blockchain ensures the integrity of the ledger. It is an immutable series of transactions shared by all participants in the ledger. Cryptographic signatures ensure correctness and guarantee “non-repudiation” (that is, once a transaction is committed to the blockchain, it cannot be un-committed). Distributed consensus algorithms ensure all participants see the same series of transactions even if bad actors try to compromise the system.

Blockchain technologies can provide a significant contribution to the improvement of efficiency and integrity in transactions in a variety of areas, including finance and healthcare. In addition, elements of blockchain technologies have been tested in a variety of use cases and contexts, including e-government and health data protection, notary services, supply chain; secure contracting and document delivery; identity; real estate systems, and many more. In order to ensure successful incorporation of blockchain in various technology ecosystems, it is necessary to improve reliability, scalability, security and privacy.

These goals cannot be achieved without the support of the features in hardware. Intel has been paying close attention to the developments in blockchain. Intel is developing products for blockchain and participating in blockchain ecosystem development via a number of initiatives, including the Linux Foundation’s Hyperledger¹⁰, the Ethereum Enterprise Alliance and an Intel’s open source distributed ledger¹¹. Intel is testing its open source distributed ledger in proof-of-concept (POC) environments in partnership with various external companies to improve the integrity and applicability of the technology. Intel’s focus has been on developing hardware functionality that will make it possible to operate blockchains on a commercial scale with greater security and support for privacy, thus creating promise for commercial deployment in several segments.

While the core capabilities of blockchain add tremendous efficiency and de-centralized authorization of transactions, these same properties, like many other innovations, have also been used for nefarious purposes. Blockchain enabled crypto-currencies, such as Bitcoin, are the preferred financial instrument of cybercriminals fo-

¹⁰ <https://www.hyperledger.org/>

¹¹ <http://intelledger.github.io/0.8/>

cused on executing ransomware. Ransomware is an efficient cybercrime in which criminals are paid directly by the victim. From the cybercriminal's perspective, there is no need to digitally fence stolen data or worry about data becoming devalued (such as stolen credit card numbers being canceled).

A typical ransomware scenario occurs when a cybercriminal gains access to a victim's (individual or organization) system and encrypts data that has value to the victim. The victim is then informed that their data is being cryptographically held hostage, and if they want their data back, they must pay a ransom. Ransom is typically paid in cryptocurrency based on blockchain, such as bitcoin, as it is easy to move the funds multiple times and difficult to map the underlying holder of a bitcoin wallet to a true individual. Ironically, market forces encourage cybercriminals to uphold their end of the bargain and typically do provide keys after payment to uphold the reputation of the ransomware model. Ransomware became practical when the usability of cryptocurrencies reached a level that victims were technically competent enough to use the system to make a payment.

We see an interesting phenomenon in ransomware in that cybercriminals appear to be moving to harder targets as profit pools dry up on soft targets. Ransomware started by targeting consumers, then moved to soft target organizations such as hospitals, police stations and universities. We now see ransomware impacting corporations and organizations. This is a worrisome trend in that critical infrastructure now presents incentives to not only be targeted by terrorists and nation-states, but also by cybercriminals. Nation states are cautious about actively attacking critical infrastructure as an attributed response could cause an undesirable reciprocal response. As it becomes more difficult to monetize consumers and organizations, cyber criminals could see a path to hold power, water or other critical systems for ransom by demanding payment by the government. We should understand these scenarios and work to understand potential policy impacts and coordinated responses prior to these scenarios playing out.

Quantum Computing

Quantum computing is a form of computing that relies on the principles of quantum physics to solve specialized classes of mathematical problems that are not practical to solve on traditional computers. Quantum computers use quantum bits (qubits), unlike digital computers, which are based on transistors and require data to be encoded into binary digits (bits). These qubits can exist in multiple states simultaneously, offering the potential to compute a large number of calculations in parallel, speeding time to resolution.

It should be noted that quantum computers will not replace traditional computers, as they are only effective on certain classes of problems, and in many cases perform worse than traditional computing. However, quantum computing holds the promise of solving complex problems that are practically insurmountable today, including intricate simulations such as large-scale financial analysis and more effective drug development. It is an area of research Intel has been exploring because it has the potential to augment the capabilities of tomorrow's high performance computers.

Another type of mathematical task that quantum computers are uniquely qualified to focus on relates to being able to break certain cryptographic algorithms. Today, data protection relies on a set of algorithms that secures everything from web connections to critical data stored or transferred in organizations or governments around the world. Some of these algorithms are called "quantum safe," meaning the mathematics of the algorithm are not subject to attack by a quantum architecture. An example of a quantum safe algorithm is the symmetric AES algorithm used for bulk data encryption. Algorithms that are "quantum unsafe" have properties that would create high levels of risk that a future quantum architecture could break the encryption. An example of a quantum un-safe algorithm is the public key algorithm RSA. Unfortunately, most encryption uses these algorithms in combination, and being able to break either one places data at risk.

One might ask why we need to think about this now if the ability to have a practical quantum computer is still years off. The reason is that encrypted data today can be "put on the shelf" by enemy nations and bad actors who will wait for the technology to mature. We must start to ask, "how long must data remain secure or secret?" If the answer is one or two years, we are fine using current algorithms. For data that must be kept secret for decades or longer, now is the time to start the transition to quantum safe algorithms.

No one company or organization will succeed alone in unlocking the path to advanced quantum computing. Instead, partnerships—such as the one between Intel and the QuTech institute in Delft, The Netherlands—in addition to industry collaboration will help realize the promise of such a technically complex issue.

Quantum computing is promising, but there are significant challenges to overcome. It is a subatomic scenario that requires suspending conventional wisdom around basic physics, where an electron can actually be two places at once, spinning clockwise and counterclockwise at the same time. This ambiguity is both promising and enormously complex—and of course, an incredibly exciting challenge to anyone who loves physics, as many at Intel do. How do we connect thousands of quantum bits, or qubits, together? How can we control them? How can we reliably fabricate, connect and control many more qubits? Even measuring qubit signals is going to require an entirely new class of low temperature electronics that don't exist today.

This research is on the cutting edge of silicon, architecture and software. As Intel's entire history has been built on driving innovations in the very leading edge of all three of these, we're excited about the role that our and other great minds can play in shaping this technology—which has the potential to shape the world for the better and solve problems we cannot solve today.

Policy Recommendations

Be wary of hard regulations—In cybersecurity the threat landscape changes very rapidly. The threat we deem the most serious today may not be the most important tomorrow. If regulation were to force manufacturers to guard against today's threats, tomorrow's might very well slip through the cracks. Additionally, if the government were to impose technology mandates, the result would likely be mere compliance rather than true security. Regulating in an area like cybersecurity is very tricky, and the unintended consequences could outweigh any benefits of the regulation.

Encourage public-private collaborations—It is far better for policymakers to collaborate with the private sector on a voluntary basis to develop risk-based, flexible frameworks to enhance the security of emerging technologies. A best-in-class example is the Framework for Improving Critical Infrastructure Cybersecurity, known as the NIST Cybersecurity Framework. It is widely acknowledged as a highly successful model of public-private collaboration that is being adopted by government agencies and critical infrastructure companies. The NIST approach succeeded because policymakers and the private sector defined a real need, improving the security of critical infrastructures; the process was open, NIST listened to the private sector, built trust with key stakeholders; and the final product, a flexible framework, was based on voluntary collaboration, not rigid regulations. Policymakers should keep in mind the recent successes of the NIST framework as a positive way to get to their desired outcome.

Implement Security and Privacy By Design—In addition to partnering with the private sector to develop and adopt flexible, voluntary security frameworks, policymakers should likewise champion the principle of security and privacy by design to help incent broad adoption by the key parts of the IoT, AI and quantum computing ecosystem. Proper protection of individual privacy in products does not just happen. It needs to be designed and engineered in from the beginning of the product development process. Security by design also means designing security in right from the start. Adding or 'bolting on' security features to a system, network or device after it's already up and running has inherent weaknesses and inefficiencies. IoT is a great example where security and privacy protections need to be designed in from the start. Attributes such as location, activities, health monitoring, finance, etc. need protection from access and disclosure unless granted by the owner. AI applications need an architecture from the beginning that allows access to high valued data while protecting the private information it may be based upon. The use of AI for genetic medical research is an example where privacy considerations are critical to both protecting patients' privacy, while allowing researchers' access to valuable data for them to validate hypotheses.

Cybersecurity and privacy must be built into the innovative equipment, systems and networks at the very start of the design and manufacturing process. Both privacy and security must be intrinsic to a product development organization's thought processes, its business processes, and its design, development, and manufacturing processes. Both privacy and security must be embedded in a product or network element so they become integral parts of the product's or element's functioning. This approach is not only more effective; it is less cumbersome and less expensive than trying to lock down systems that are leaking personal information or are inherently insecure.

Revise Vulnerabilities Equities Process—As with all technologies and more so with emerging technologies, vulnerabilities will arise that need to be corrected to assure proper operation of the solution, assuring its safety and security. The issue of vulnerability disclosure has been a subject of debate for some time. Currently there are concerns about how the U.S. Government deals with zero-day vulnerabilities that

its agencies, and those acting on its behalf, discover. The government should revise its vulnerability equities review and disclosure policies to allow greater transparency on how the government is implementing the vulnerabilities equities process. A revised policy would do much to enhance trust in the IT eco-system, something particularly important in the context of the emerging technologies we have been discussing today.

Conclusion

It has been an honor to testify before such a distinguished panel of legislators. We face a cybersecurity threat landscape that is constantly evolving with each new technology that is brought to market at a faster pace than ever before. Rapid advances in hardware and software are creating new categories of innovative technologies such as the Internet of Things, artificial intelligence, quantum computing, and blockchain algorithms.

All of these innovative technologies merit attention from policymakers given their potential to solve complex problems, grow new markets and create high wage jobs. At the same time, these innovations can also create new security challenges and opportunities that need to be addressed in a thoughtful, prudent manner. Toward that end, we encourage policymakers to partner with the private sector to develop flexible, voluntary and market-based solutions, rather using regulatory models to address the challenges of emerging, innovative technologies. Policymakers are in a position to incent the ecosystem of emerging technology providers to adhere to the principle of security by design. By working together, policymakers and the private sector can harness the benefits of innovation while also addressing its challenges.

The CHAIRMAN. Thank you, Mr. Grobman.
Mr. Harkins?

STATEMENT OF MALCOLM HARKINS, CHIEF SECURITY AND TRUST OFFICER, CYLANCE INC.

Mr. HARKINS. Thank you, Chairman Thune, Ranking Member Nelson, and others of the Committee. I'm Malcolm Harkins, Chief Security and Trust Officer with Cylance Corporation.

I'd like to start by telling you a story that I think will add some perspective to the promise and the peril of emerging technologies. The story starts in 2013 when the FDA approved an experimental eye surgery: high-tech sunglasses with a camera, video processing unit, a graphics processing unit, small operating system, a retinal implant.

In June 2015, a 59-year-old gentleman in Ohio had that surgery. The concept was that with computing and with capabilities, we could perhaps transform this person's life, change their outcome, get them to regain their sight. That's the hope and the promise of technology. That's what computing can do, to connect and enrich lives, to create social benefit, to create economic benefit.

Now, what happened in June 2015 when he had that surgery—several weeks, a couple of months later—and I'll quote from him—"The other day, I asked my wife, Karen, to point me to the Moon to see if I could see it. I couldn't. But I turned around and I suddenly saw her face." That is what computing can do for us if we do it right. But the one thing that's true about computing is any device that computes can also execute code, which means it has the potential to execute malicious code.

Now, imagine that visor, those high-tech sunglasses, on that gentleman. If it was poorly designed, developed, and implemented, and it had the ability to execute malicious code, and you hold a QR code in front of that person's face, you flip bits, and they get held hostage to paying Bitcoin to get their eyesight back. That's the peril.

You know, we have problems today in the world that we're facing. We see them day in and day out across the headlines. I believe we can't solve tomorrow's problems until we look at the problems we have today. Otherwise, we'll carry forward the risk issues that we're seeing today.

Having run risk and security in a large enterprise as well as a small enterprise now for 16-plus years, I can tell you there are two battlefields that the Chief Information Security Officer or Chief Security Officer faces in an organization today. There's the external battlefield that we see day in and day out. We see in the press, the threat actors and the threat agents that are coming after us.

But let's look at some of the data on that external battlefield. A recent ISSA survey said that 45 percent of cybersecurity professionals, the people that run security in their organizations, said their organizations are significantly vulnerable, and 47 percent said they're somewhat vulnerable. Ninety-two percent of the cybersecurity professionals in organizations think that their organizations are vulnerable.

Another recent survey: 61 percent of organizations today have ransomware in their organization. Another survey from Europol on the Internet Organized Crime Threat Assessment Report—their look at all the investigations they've done over the past couple of years—the majority of attacks are neither sophisticated nor advanced. Techniques are re-used, re-cycled, and re-introduced.

On the internal battlefield, again, some additional surveys. Twenty-one percent of chief information security officers say that executive management treats cyber risk as a low priority. Sixty-one percent of the turnover for chief information security officers, which happens about every 2 to 3 years, is predominantly because of the lack of a serious cybersecurity culture in their organizations.

Now, I don't believe all is lost. I think there's hope. I think there's promise. We can do better. Dr. Paul Sieving, the Director of the National Eye Institute in the National Institutes of Health, said in September of 2015 after the surgeries to get people back their vision, "When you know the cause of something, you can begin to think about how to ameliorate it." We know the cause. We know the cure. We can put better security development, lifecycle and privacy by design to lower the vulnerabilities in technology prior to its implementation.

We also know the cure for today's problem. We can leverage advances in artificial intelligence and machine learning. Cylance is doing that today. We've already proven that we can unlock the DNA, have an atomic level of malicious code, and preempt prior to the execution of code its ability to do harm. We can do it in milliseconds.

I think if we step back and look at all these things, and we put ourselves in a better position to drive business outcomes for the promise of technology, we'll be better apt to avoid the peril. And I think if we do that, and do that right, we can do three things. We can create a demonstrable and sustainable bend in the curve of risk. We can lower the total cost of controls in organizations that's growing unchecked and unmitigated, just like the risks are. And we can reduce the control friction that gets created because the security solutions that are deployed today disrupt the ability to

compute, they disrupt the user experience, and they become a drag coefficient on the business velocity of organizations.

Thank you.

[The prepared statement of Mr. Harkins follows:]

PREPARED STATEMENT OF MALCOLM HARKINS, CHIEF SECURITY AND TRUST OFFICER, CYLANCE INC.

Good morning Chairman Thune, Ranking Member Nelson, and other members of the Committee. Thank you for the opportunity to testify today. I am Malcolm Harkins, Chief Security and Trust Officer for Cylance Inc. I am pleased to address the Committee on how emerging technologies such as artificial intelligence, the Internet of things, blockchain (the technology behind Bitcoin), and quantum computing will drive a new generation of cyber vulnerabilities. Every evolution of technology holds the promise of innovation and creates unique security risks. However, with the proper design and forward looking considerations these emerging technologies can also be used to combat cyber threats more effectively.

My testimony will focus on the following areas

- The innovation cycle and how that is fueling emerging technologies which are leading to digital transformations that present tremendous opportunity for economic as well as societal benefit.
- The information risk and security implications for these emerging technologies. The potential impacts and concerns to individuals, business, and government agencies if the creators do not provide proper security capabilities as they design, develop, implement, and maintain these new innovations.
- The cybersecurity opportunities these technologies offer to enable better risk mitigation thru prevention rather than today's norm of react and response.
- How we should be framing the digital opportunities in front of us so that we can achieve digital transformation and digital safety to ensure tomorrow is better than today.

First, I would like to provide some background on my experience and Cylance's commitment to cybersecurity.

As Chief Security and Trust Officer for Cylance, I am responsible for enabling business growth through trusted infrastructure, systems, business processes and staff training. I have direct organizational responsibility for information technology, information risk and security, as well as security and privacy policy. I am also responsible for peer outreach activities to drive improvements and understanding of cyber risks. I work with business leaders, industry peers, security experts and regulatory partners to develop best practices for managing and mitigating those risks.

Prior to joining Cylance in 2015, I spent almost 24 years at Intel Corporation. My last role at Intel, which I held for more than 2 years was Vice President and Chief Security and Privacy Officer (CSPO). In that role, I was responsible for managing the risk, controls, privacy, security, and other related compliance activities for all of Intel's information assets, products, and services. Before becoming Intel's first CSPO, I was the Chief Information Security Officer (CISO) reporting into the Chief Information Officer. Over my years at Intel I also held roles in Finance, Procurement, and other business operational positions.

I have been fortunate to receive both peer and industry recognition over the years including the RSA Excellence in the Field of Security Practices Award, Computerworld Premier 100 Information Technology Leaders, Top 10 Break-away Leaders at the Global CISO Executive Summit, and the Security Advisor Alliance Excellence in Innovation Award. I have authored many white papers, blogs, and articles. In December 2012 I published my first book, Managing Risk and Information Security: Protect to Enable®. I was also a contributing author to Introduction to IT Privacy, published in 2014 by the International Association of Privacy Professionals. The 2nd edition of my book, Managing Risk and Information Security: Protect to Enable®, was recently published in August of 2016.

Cylance's Commitment to Cybersecurity

Cylance was founded in 2012 by Stuart McClure and Ryan Permeah with the sole purpose of revolutionizing cybersecurity by replacing outdated reactionary security models with proactive prevention based security using artificial intelligence and machine learning to stop attacks before they occur.

Stuart McClure previously served as the Global CTO of McAfee/Intel Security business and is the founding/lead author of the international best-selling book Hack-

ing Exposed. Ryan Permeh previously served as Chief Scientist at McAfee/Intel Security and is the brain behind Cylance's mathematical architecture and new approach to security. In building Cylance, Mr. McClure and Mr. Permeh brought together the best data science, security and executive minds from the likes of Cisco, Sourcefire, Google, Symantec, McAfee and several Federal intelligence and law enforcement agencies to create a new security model that is focused on prediction of attacks and preventing them from occurring.

Cylance® is the first company to apply artificial intelligence, algorithmic science, and machine learning to cybersecurity and improve the way companies, governments, and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist. By coupling sophisticated artificial intelligence and machine learning with a unique understanding of an attacker's mentality, Cylance provides the technology and services to be truly predictive and preventive.

Leveraging cutting-edge artificial intelligence and machine learning, our flagship product CylancePROTECT offers future-proof prediction and prevention of the most advanced threats in the world including advanced persistent threats, zero-days, and exotic exploitation techniques never seen before. CylancePROTECT also guards from everyday viruses, worms, ransomware, spyware/adware, Trojan horse attacks and spam.

The problem with legacy security solutions is that adversaries can continually evolve their techniques and tactics to bypass them, leaving enterprises exposed to attacks. This means that traditional solutions are reactive in nature and rely on a constant stream of "signature updates" that tell these solutions what type of files to look for after an attack was successful on some other system, these are called "zero-day" attacks. Traditional security solutions are built around a basic set of rules and signature files that are costly and high risk because they require a zero-day "sacrificial lamb" before they can create the ability to block an attack, meaning it is not possible to identify a new threat until after the damage is done. But CylancePROTECT is different—it can identify and defuse even never-before-seen attacks prior to execution. This means that we can stop new variations of attacks without a zero-day sacrificial lamb. Our AI-based solution is flexible and can support new generations of technologies such as the Internet of things and many others.

Our commitment to cybersecurity was well demonstrated and documented in September 2016 House Oversight committee report on the OPM data breach. "The committee obtained documents and testimony that show internal bureaucracy and agency politics trumped security decisions, and that swifter action by OPM to harden the defenses of its enterprise architecture by deploying PROTECT would have prevented or mitigated the damage that OPM's systems incurred." OPM IT Security Officer Jeff Wagner said in an e-mail that Cylance was able to find things that other tools could not "because of the unique way that Cylance functions and operates. It doesn't utilize a standard signature or heuristics or indicators, like normal signatures in the past have been done. It utilizes a unique proprietary method." The effectiveness of Cylance at OPM meant that upon our engagement in less than 10 days 2,000+ pieces of malware were identified that had previously not been stopped or detected across 10,000+ hosts that are now protected by CylancePROTECT.

The Innovation Cycle Of Emerging Technologies

Understanding these innovations and the digital opportunities they offer

The march of technology can be viewed as a succession of major waves, each lasting roughly 100 years (Rifkin 2013). Each wave has brought transformative benefits to society, but also significant challenges. The first wave, starting in the 1760s, included steam power, railways, and early factories as well as mass education and printing. The second wave, starting roughly in the 1860s and continuing well past the mid-1900s, included automobiles, electricity, mass production, and had an even bigger effect on society.

Version 1.0: 1760s

Steam and coal
Railways
Factories
Printing press
Mass education

Version 2.0: 1860s

Electric lights
Communications
Oil & gas
Mass production
Automobiles

Version 3.0: 1990s

The Internet
Molecular biology
Renewable energy
"Smart" everything

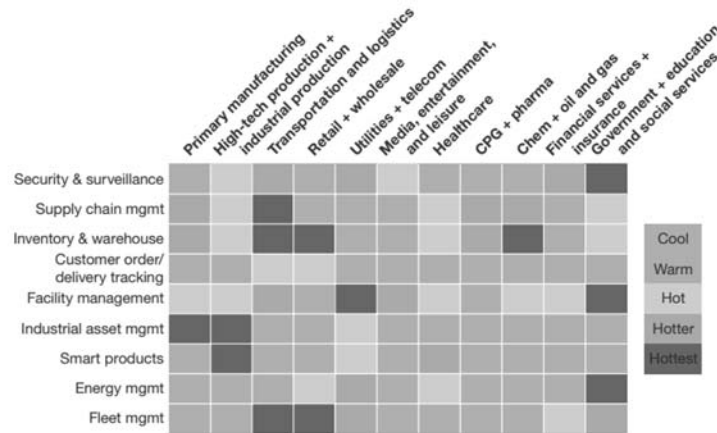
The third wave began in the 1960s, with early computers, but only really gained momentum in the 1990s. It includes the Internet and smart “things”, molecular biology and genetic engineering, and renewable energy. Arguably, this technology wave may have the broadest impact on society of any to date. Each previous wave lasted about 100 years, so history suggests that we are far from reaching the crest. To provide some perspective—if we thought of this wave as a movie, we’d still be watching the opening credits.

The Internet of Things (IoT) has come upon us at a fast and furious pace. It gets discussed and hyped constantly, but sometimes without a clear definition. And, as such, the phrase can mean different things to different people. But a simple way to think about it is that any powered device will compute, communicate, and have an IP address—meaning it is connected to a network. The Internet of things allow devices to be sensed or controlled remotely across the Internet. This has created opportunities for more direct integration of the physical world into computer systems. When IoT is augmented with various sensors we have what is often defined as smart grids, smart homes, and smart cities. Each IoT device has an embedded computing system and is able to interoperate within the existing Internet infrastructure. Many estimate indicate that the IoT will consist of more than 50 billion devices by 2020, some estimates top 70 billion devices.

IoT devices or objects can refer to a wide variety applications including everything from a heart monitoring implant or pacemaker to biochip transponders on farm animals or children’s toys such as an Internet connected Barbie doll. Current market examples include home automation, such as Google Nest, which can provide control and automation of lighting, heating, ventilation, air conditioning (HVAC) systems, and appliances such as washer/dryers, robotic vacuums, air purifiers, ovens or refrigerators/freezers that use Wi-Fi for remote monitoring.

In November of 2016, Louis Columbus from Forbe’s wrote, “This years’ series of Internet of Things (IoT) and Industrial Internet of Things (IIoT) forecasts reflect a growing focus on driving results using sensor-based data and creating analytically rich data sets. What emerges is a glimpse into where IoT and IIoT can deliver the most value, and that’s in solving complex logistics, manufacturing, services, and supply chain problems.”

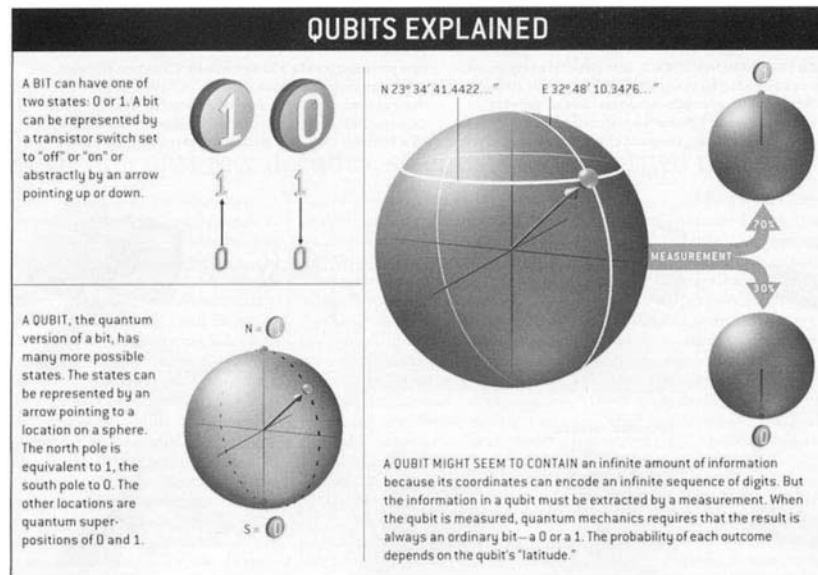
FIGURE 6 Heat Map Of Key IoT Opportunities Varies By Industry And Application



Source: Forrester—The Internet Of Things Heat Map 2016, Where IoT Will Have The Biggest Impact On Digital Business by Michele Pelino and Frank E. Gillett January 14, 2016

Quantum Computing is also emerging quickly. In 2011 Microsoft created a Quantum Architectures and Computation Group with a mission to advance the understanding of quantum computing, its applications and implementation models. In February 2017, Brian Krzanich, CEO of Intel said he was “investing heavily” in quantum computing during a question-and-answer session at the company’s investor day. Earlier this month in March 2017, IBM announced that it’s planning to create the first commercially-minded universal quantum computer.

Today's computers work by manipulating bits that exist in one of two states: a 0 or a 1. Quantum computers aren't limited to two states. By harnessing and exploiting the laws of quantum mechanics to process information a quantum computer can encode bits which contain these multiple states simultaneously and are referred to as Quantum bits or "qubits". Quantum computing has the potential to be millions of times more powerful than today's most powerful supercomputers. Last year, a team of Google and NASA scientists discovered a D-wave quantum computer was 100 million times faster than a conventional computer.

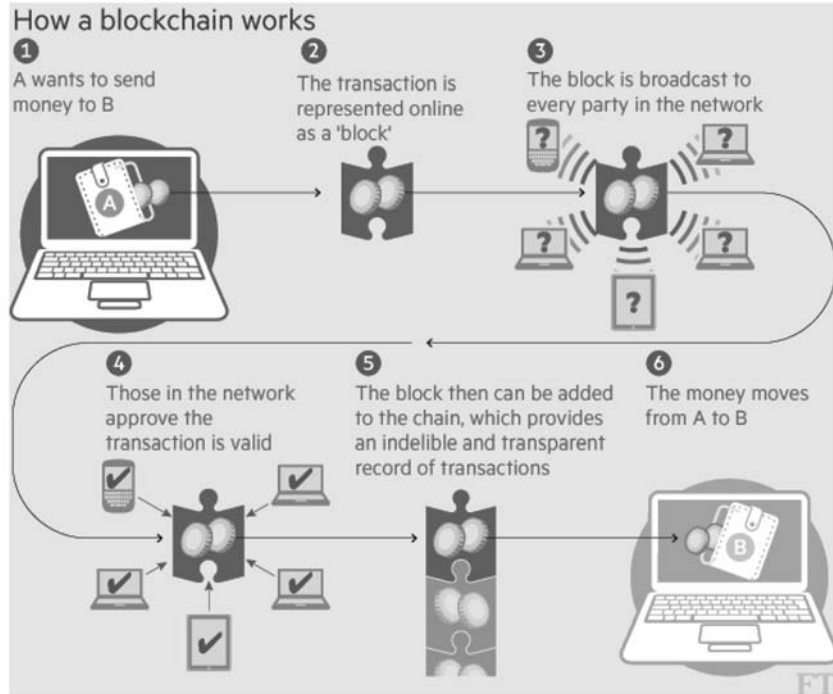


Source: Universe Review

This means that many computing challenges and difficult computation tasks, long to be thought impossible (or "intractable") for classical computers will be achieved quickly and efficiently by a quantum computing. This type of leap forward in computing could allow for not only faster analysis and computation across significantly larger data sets. It would reduce the time to discovery for many business, intelligence and scientific challenges which include improving energy grids, protecting and encrypting data, simulations of molecules, research into new materials, development of new drugs, or understanding economic catalysts. Quantum Computing can reduce time spent on physical experiments and scientific dead ends resulting lower costs and faster solutions that can provide economic and societal benefit.

Blockchain as many people know it is the technology behind Bitcoin. A blockchain is a distributed database that maintains a continuously growing list of ordered records called blocks. Each block contains a timestamp and a link to a previous block. By design, blockchains are inherently resistant to modification of the data. Once recorded, the data in a block cannot be altered retroactively. Blockchains are an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically.

The technology can work for almost every type of transaction involving value, including money, goods and property. Its potential uses are wide ranging: from collecting taxes to more effectively managing medical records to anything else that requires proving data provenance.



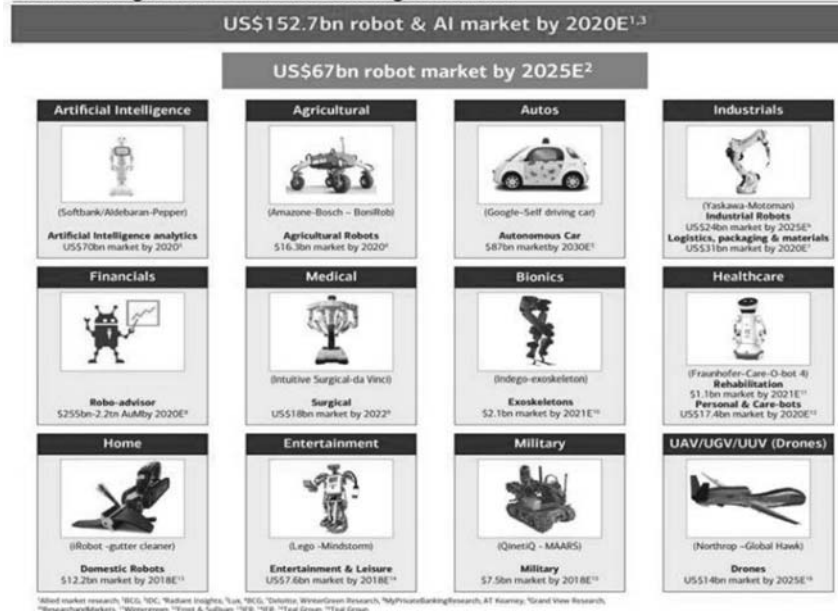
Source: WEFORUM.ORG

Artificial Intelligence is progressing rapidly with everything from SIRI to self-driving cars relying on it automate specific tasks. While there is a wide variety of definitions of AI. Artificial intelligence today is properly known as narrow AI (or weak AI), in that it is designed to perform a narrow task (e.g., only facial recognition or only Internet searches or only driving a car). However, the long-term goal of many researchers is to create general AI (or strong AI). While narrow AI may outperform humans at whatever its specific task is, like playing chess or solving equations, general AI would outperform humans at nearly every cognitive task.

Machine learning is a branch of artificial intelligence (AI). Machine learning is also one of the most important technical approaches to AI. It is the basis of many recent advances and commercial applications of AI. Machine learning is a statistical process that starts with a body of data and tries to derive a rule or procedure that explains the data or can predict future data.

A simple way to describe how ML works is as follows: In traditional programming, you give the computer an input—let's say $1+1$. The computer would run an algorithm created by a human to calculate the answer and return the output. In this case, the output would be 2. Here's the crucial difference. In machine learning, you would instead provide the computer with the input AND the output ($1+1=2$). You'd then let the computer create an algorithm by itself that would generate the output from the input. In essence, you're giving the computer all the information it needs to learn for itself how to extrapolate an output from the input. In classrooms, it's often stated that the goal of education is not so much to give a growing child all the answers, but to teach them to think for themselves. This is precisely how machine learning works.

AI has applications in everything from Agriculture for crop monitoring, automated irrigation/harvesting (GPS-Enabled) Systems to the Media and Advertising industry with Facial Recognition Advertising.

Exhibit 1: The global robots & artificial intelligence market

Source: BofA Merrill Lynch Global Research

The Information Risk and Security Implications

The digital disasters that could be created if we don't manage the risks ahead

These days, it's hard to read an online news source, pick up a newspaper, or watch TV without seeing reports of new threats: cybercrimes, data breaches, industrial espionage, and potential destruction of national infrastructure. These reports inevitably leave the impression that we are drowning in an inexorable tide of new and terrifying threats. Reports such as; "CloudPets' woes worsen: Webpages can turn kids' stuffed toys into intrusive audio bugs" read the headline on March 1, 2017 posted on The Register by Richard Chirgin. "Fatal flaws in ten pacemakers make for Denial of Life attacks" wrote Darren Pauli on December 1, 2016. Whether it is these headlines or the ones from June 2015 reporting "that hacker's show how to remotely crash a Jeep from 10 miles away" or the countless other headlines communicating vulnerabilities found or the breaches that have occurred, there is one common denominator that exists today and will exist tomorrow. Any device that executes code has the ability to be compromised and execute malicious code.

Emerging technology such as IoT, Blockchain, quantum computing, and artificial intelligence offer tremendous promise for benefit, but if poorly designed, developed, and implemented and there is a likely ability to execute malicious code harm will occur. The variety of risks and impacts to individuals, to our businesses, the economy, and potentially to society could be wide ranging and financial significant.

When assessing risk, I think it is important to look at data. Here is some data from recent surveys and studies:

2016 Europol Internet Organized Crime Threat Assessment Report

- Increase acceleration of previous threat and vulnerability trends
- APT and cybercrime boundaries blur
- Majority of attacks are neither sophisticated nor advanced: techniques are re-used, recycled, and re-introduced
- Investing in prevention may be more effective than investigating

2016–2017 National Association of Corporate Directors Public Company Governance Survey

- Cybersecurity threats are expected to have the fifth greatest effect on a company in the next 12 months
- 75 percent of respondents report short term performance pressures compromise management and the board's ability to focus on the long-term
- Directors continue to wrestle with effective oversight of cyber risk. Many of them lack confidence that their companies are properly secured and acknowledge that their boards do not possess sufficient knowledge on this growing risk

ISSA—Through the Eyes of Cyber Professionals—Part 2

- 45 percent of cyber professionals think their organizations are significantly vulnerable to cyberattacks
- 47 percent think their organizations are somewhat vulnerable to cyberattacks
- 40 percent of cyber professionals want goals established for IT around cybersecurity
- 44 percent of cyber professionals indicate they do not get enough time with the board
- 21 percent say that business and executive management treat cybersecurity as a low priority
- 61 percent of CISO turnover is due to a lack of a serious cybersecurity culture and not active participation from executives

The conclusion that I can draw from this data, as well as all the headlines we see daily on breaches, including the March 9th 2017 headline from Tara Seals at Information Security Magazine that read “61 percent of Orgs Infected with Ransomware” is this: We are not in aggregate doing a good job today managing our risk. We need to do better. We have to do better. Not only do we need to make immediate improvements today we need to get in front of our future risks. Otherwise, the potential we have in front of us with technological advancements, which can benefit individuals, business, government and our society will be called into question.

We Can Do Better at Controlling for Risk Today as Well as Tomorrow

Emerging technologies, coupled with the right risk profile and control assessment frameworks enable better risk mitigation.

In the world of cybersecurity, the most frequently asked question focuses on “who” is behind a particular attack or intrusion—and may also delve into the “why”. We want to know whom the threat actor or threat agent is, whether it is a nation state, organized crime, an insider, or some organization to which we can ascribe blame for what occurred and for the damage inflicted. Those less familiar with cyberattacks may often ask, “Why did they hack me?”

These questions are rarely helpful, providing only psychological comfort, like a blanket for an anxious child, and quite often distract us from asking the one question that can really make a difference: “HOW did this happen?”

The current focus on the WHO and the WHY does the industry and everyone else in general very little service. We need to rethink and refocus the Security Risk Equation to examine how the attack occurs to prevent them in the future.

Let's start by looking at the popular “risk equation” commonly used when assessing the possibility of a breach or cyberattack:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Asset Value or Consequence/Impact}$$

As someone who has been responsible for managing information risk and security in the enterprise for 15-plus years, I have thought through this equation countless times strategically, as well as tactically, during an incident. The conclusion I have arrived at over and over and over again is that I have little control or influence over threat actors and threat agents—the “threat” part of the above equation. The primary variable I do have control over is how vulnerable I am—meaning the strength of my present as well as my future control.

From a consequence and impact perspective there are only three primary consequences we need to focus on Confidentiality, Integrity, and Availability. Each of these have different potential impacts to an individual, to an organization, or more broadly to society depending on the technology or data attacked. When we examine “how” attacks are accomplished we see three core targets for attacks:

- Attacks on identity credentials

- Attacks focused on the execution of malware
- Attacks that create a Denial of Service

So what must always be analyzed and reported on is HOW an intrusion or attack was successful, so we can give attribution to either the control(s) that failed, the lack of control(s), and to those responsible for maintaining proper control.

A great example of this sort of investigation and analysis is the House Committee on Oversight and Government Reform OPM breach report which occurred in September of 2016 and in the subsequent report published in January 2017 by the Office of the Director of National Intelligence on Background to “Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution.” There are a few important items to note from the upfront background section:

- 1) “Intelligence Community judgments often include two important elements: judgments of how likely it is that something has happened or will happen (using terms such as “likely” or “unlikely”) and confidence levels in those judgments (low, moderate, and high) that refer to the evidentiary basis, logic and reasoning, and precedents that underpin the judgments.”
- 2) The nature of cyberspace makes the attribution of cyber operations difficult, but not impossible. Every kind of cyber operation—malicious or not—leaves a trail. U.S. Intelligence Community analysts use this information, their constantly growing knowledge base of previous events and known malicious actors, and their understanding of how these malicious actors work and the tools that they use, to attempt to trace these operations back to their source.

The government—which has badges, guns, jails and laws to enforce—should continue to focus law enforcement and other government agencies on attribution related to the source(s) of attacks, so they can take action to deter (via conviction and jail time) the threat actors who wish to do harm. They can also post an incident if enough evidence exists, attempt to detain and prosecute those responsible. However, this alone is a completely insufficient forum of attribution and per the report itself, has a degree of judgment.

Learning from the History of Attribution

One thing that can be done with complete certainty is to look closely at HOW the threat actors were successful, and hold those people and organizations accountable. We can also look back in history and learn how every other reported intrusion occurred in the past decade, including the now-infamous attacks on Sony, Home Depot, OPM, Yahoo, Target, Anthem, and JPMC. This attribution is irrefutable, and the only question we now have left to answer is why the same story has presented itself over and over again, and why are we (as an industry) failing to pay attention to it.

All of these intrusions have been successful due to one or both of the following incidences occurring:

- 1) Control(s) that failed, and/or
- 2) Incomplete or lack of control(s)

We can attribute the source of these items very simply and with certainty by answering two basic questions:

- 1) Who is accountable for the control environment?
- 2) Who created the control(s) that failed?

So, whom should we really hold accountable for the success of all these intrusions? The none-too-flattering answer is that while the breached organizations or the creator of the technology that was vulnerable may shoulder some of the blame, we can attribute the success of these attacks to the in many cases to cybersecurity industry itself.

Here is the simple reason: the security industry sells controls that fail, and do so repeatedly. And here’s the rub. These products and services don’t just fail in extreme conditions or due to highly unusual or sophisticated attacks. Every one of the organizations that suffered a breach was relying on the capabilities of a security provider that failed to prevent the attack.

Why are these vectors so easy? The simple reason is that in many cases, the security solutions deployed don’t work with high enough success rate to make an attack difficult or even challenging.

Disengaging from the Blame Game

In order to move forward and refocus our industry's energies on making attacks more difficult for malicious actors, we need to break free from our own obsessive infatuation with attribution. By investing all of our resources into finding out "whodunnit," we get to play the victim card to minimize our own responsibilities and limit our liabilities. None of that helps the organizations that have been breached or the customers and clients who trusted those companies with their private information.

Instead, we need to focus on WHY those intrusions were successful, so we can give attribution to the real source of the intrusion—the controls that failed or lack of control.

This form of attribution will bring real accountability, and recalibrate our collective sights to take aim at the one variable in the risk equation that we have real influence over—our strength of control. Then, and only then, can we start to make a difference and put a bend in the curve of risk we have been witnessing, versus continuing to let it grow unchecked.

Control frameworks that add value

I have said for years that the core of business-driven security and the mission of the information risk and security team is "Protect to Enable." When you are protecting to enable people, data, and the business, you are proactively engaged upfront and aligned with the business on the evaluation of how to achieve the business objective, while best optimizing your controls.

I achieve that through my "9 Box of Controls" approach that was published in September of 2016 in the second edition of my book—*Managing Risk and Information Security: Protect to Enable*. Let me explain my perspective on controls. My perspective is rooted in my experiences as a business leader and in my many years in Finance, including my role as a profit and loss manager for a billion dollar business unit in the late 90s. It is a control philosophy that I have carried forward in my roles in security, but one that I believe is lacking in the industry.

An important aspect of this perspective is the concept of control friction. I've developed a simple framework called the 9 Box of Controls, which takes the issue of control friction into account when assessing the value as well as the impact of any control, including information security.

I believe that the 9 Box of Controls includes some actionable perspective that may be valuable to many organizations facing these universal risk challenges. My conversations with peers at other companies have validated this view. Many of them are now using the 9 Box to drive not only tactical, but also strategic discussions in their organizations around where they are spending their resources today, and where they should be headed long term.

Types of Security Controls

There are three primary types of security controls: prevention, detection and response:

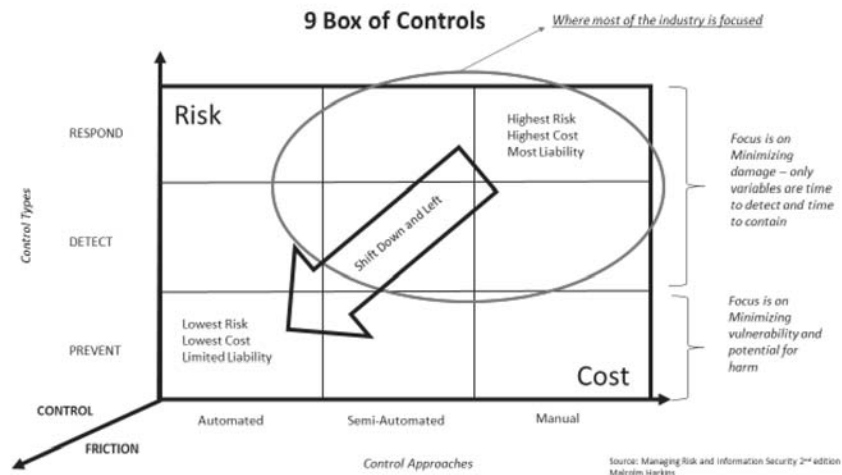
- Prevention occurs when an action or control prevents a vulnerability up front in the design and development, or prevents an infection or cyberattack in its tracks before it affects users or the environment
- Detection means identifying the presence of a vulnerability or detecting something malicious that has already entered the environment
- Response is a reaction to the discovery of a piece of malicious code, attempting to remove it after it has already affected the user or the organization

From a risk perspective, prevention focuses on minimizing vulnerability and the potential for harm, while detection and response focus on minimizing damage. When you are focused on minimizing damage, the main variables to turn the reactive risk dials are (a) time to detect and (b) time to contain.

There are also three primary approaches one can take to implement a control: automated, semi-automated, and manual.

- Automated control occurs entirely through machines
- Semi-automated control involves some level of human intervention
- Manual controls are managed entirely by hand

The combinations of these control types and automation levels comprise the cells of the 9 Box, as shown in the figure below. Risk increases as we move from prevention, to detection, to response. Cost increases as we move from automated to semi-automated to manual controls.



A Note on Control Friction

However, there is a third dimension to the 9 Box: control friction. As we know, friction is the force that causes a moving object to slow down when it comes into contact with another object. Similarly, controls can impose a “drag coefficient” on business velocity—they can slow the user or a business process. Just think of the groan issued by PC users when they switch on their machine to complete an urgent task, only to find it indisposed for the next half hour due to a patch or virus scan. Or think of the impact on time to market if your design or development practices are bogged down with slow and cumbersome security development lifecycle or privacy by design efforts.

However, friction is not a fundamental, immutable force like gravity or electromagnetism. Instead, we have the ability to determine exactly how much control friction we apply. Apply too much control friction, and business users may choose to circumvent IT security controls or the product security controls in the upfront design of technology. This adds not only cost but it also adds risk: because the security team lacks visibility into the technology being created or used. So it cannot prevent vulnerabilities or compromises, detection becomes difficult due to lack of visibility, and in many cases, response after the fact becomes the only option.

If a business adheres to high-friction controls, the long-term effect can be the generation of systemic business risk. High-friction controls can hinder business velocity; the organization can lose time to market and the ability to innovate, and over the long term it may even lose market leadership.

Implementing the NIST (National Institute of Standards and Technology) Cybersecurity Framework and continuously walking through the macro steps that it outlines is also another approach we should all continue to adopt and promote.

- Prevention Steps: Identify and Protect.
- Reaction Steps: Detect, Respond, and Recover.

If implemented properly, the NIST framework can set the stage for having the right discussion within an organization on information risk. It can also, when viewed in the context of the 9 Box of Controls, drive a “shift left and shift down” to better enablement, which results in the lowest risk, lowest cost, least amount of liability, and lowest control friction spot—so we can all “Protect to Enable” not only our organizations for today and tomorrow but also our customers.

I also hope that with the right discussion we can all focus on “not” positioning the work of managing risk as an “either this or that” function. We need to recognize and remember compliance does not equal security. We need to avoid positioning business velocity vs. business control. We need to avoid positioning privacy as a balancing act against the need for security. If we start with a mindset of trading these items off against each other, we will not be successful, because we will design our digital transformation to be at odds with the digital control needed to do this right.

And then, we will be left with throwing money at symptoms after the fact, reactively detecting and responding to risk rather than fixing the problem from the ground up.

How emerging technologies can help

Any future security architecture we implement must provide better prevention, and it must also be more flexible, dynamic, and more granular than traditional security models. A new architecture also needs to greatly improve threat management. We need to do this in the upfront design, development, and validation during the creation of technology to reduce vulnerabilities well before the technology gets deployed. And as new attacks appear, we need a security system that is able to recognize good from bad in milliseconds, so that it can stop the bad and allow the good. For any attack that gets past these preventive controls, we need to be able to learn as much as we possibly can without compromising the user's computing performance or privacy. This information enables us to investigate exactly what occurred, so we can take immediate action to mitigate the risk whilst also learning how to prevent similar attacks in the future.

A control architecture should assume that attempts at compromise are inevitable—but we should also understand that it is possible to achieve real prevention for 99 percent or more of risks that could occur, including that of malicious code and zero-day attacks caused by mutated malware. Should a piece of malicious code attempt to execute, we can then instantly apply artificial intelligence and machine learning to analyze the features of files, executables, and binaries to stop the code dead in its tracks before it has a chance to harm the environment. For the remaining attacks—representing less than 1 percent of malware—we need to focus heavily on survivability.

Blockchain as explained early has significant value well beyond the implications a new form of money. By design, blockchains are inherently resistant to modification of the data. Once recorded, the data in a block cannot be altered retroactively. The implications then to use blockchains as a method to overcome many of the current weaknesses and vulnerabilities of the Internet and usher in a new age of trusted secure transactions is significant.

Quantum computing also offers exciting possibilities to enhance security as well. As mentioned earlier this type of leap forward in computing could allow for not only faster analysis and computation but across more data sets. Reducing the time to discovery in simulations can be used not only to aid research into things like new materials, drugs, or industrial catalysts. The tactic can reduce time spent on finding vulnerabilities in the design and development cycle for technology. This will then lower control friction on the developers of technology and increase the probability that they can find and fix a vulnerability prior to deployment. Doing so will not only lower secure design costs, it will speed up an organizations time to market with technology that is inherently less vulnerable to attack. The final result will be a broad reduction of societal and individual risks.

Artificial intelligence and more specifically machine learning are here today and Cylance is already demonstrating the impact it can have. As I mentioned in the initial section of my testimony Cylance is the first company to apply artificial intelligence, algorithmic science, and machine learning to cybersecurity and improve the way companies, governments, and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist. By coupling sophisticated artificial intelligence and machine learning with a unique understanding of an attacker's mentality, Cylance provides the technology and services to be truly predictive and preventive.

In the future artificial intelligence and machine learning will also be able to solve other vexing issues that we face today such as passwords and identity management used to authenticate and authorize users. We will also be able to mitigate distributed denial of service attacks using the ability to predict and thus prevent in automated fashion the flood of requests that can so easily disrupt an organization today.

JFK once said, "The problems of the world cannot be solved by skeptics or cynics whose horizons are limited by the obvious realities. We need men who can dream of things that never were and ask why not." When AI, quantum computing, and blockchain are combined with right approach and right architecture the reduction in risk, the reduction on the cost of control, and the reduction in the control friction experienced by users and business will be dramatic.

Making Sure Tomorrow Is Better Than Today

The Perils and the Promise of Emerging Technologies for Cybersecurity

I read an article by Forbes leadership advisor and author Mike Myatt just a few weeks ago. I was reminded of something I was told a long time ago; “If there is a conversation you have been avoiding, that’s the one to have.”

I think there is a broader conversation that we as a security industry, as well as a tech industry, have avoided, and in some cases have intentionally distracted others away from having. In reality, there are two discussions—one for the creators/users of technology and one for the security industry. Both share a common conclusion that results in harm to others. Beyond that, both problems have a path forward that can address these failings.

What Every CEO Should Know

Myatt wrote a great piece last month titled Digital Transformation or Digital Free Fall: What Every CEO Must Know.

In the article, he astutely explains, “Innovation has always been synonymous with business survival and that hasn’t changed. What has changed is the pace and scale at which businesses must innovate to remain competitive in a digital world. The speed of technology advances in the market are making the old paradigm of first mover versus fast follower largely irrelevant—every business must now become some version of a first mover.”

He also goes on to point out that “Digital transformation is really more of a leadership, culture, strategy, and talent issue than a technology issue. Real digital transformation occurs when business models and methods are reimaged by courageous leaders willing to manage opportunity more than risk, focus on next practices more than best practices and who are committed to beating their competition to the future.”

In my second book, I published a set of 9 Irrefutable Laws of Information Risk. Law #9 states: “As our digital opportunities grow, so does our obligation to do the right thing.” I believe this is a crucial point that was left out of Myatt’s piece.

Courageous leaders in digital transformation realize that business survival is also about managing risk, not just managing or chasing opportunity. Too many organizations today are chasing digital opportunities while risking their customers, and in some cases, society. Richard Rushing, CISO at Motorola Mobility, posted in December a picture from a presentation that read, “We’re building self-driving cars and planning Mars missions—but we haven’t even figured out how to make sure people’s vacuum cleaners won’t join botnets.”

The Real Life Implications of Digital Transformation

Digital transformation as discussed throughout my testimony is embedding technology into the fabric of our lives. Typically, these technologies are meant to help or assist users, but one key element is often overlooked: Exploits that take advantage of technological vulnerabilities will increasingly impact the well-being of almost everyone in our society. So, it is incumbent upon all of us to properly shape the way we design, develop, and implement digital transformations to best manage and mitigate the information security, privacy, and other risks that are being generated, while still challenging ourselves to create technology that helps people.

The World Economic Forum 2017 Global Risk Report had Cyber Dependence in its top five risk trends, just below climate change and polarization of societies. It also indicated that “. . . technology is a source of disruption and polarization.” I also believe technology is a tremendous opportunity for economic and societal benefit. I believe that technology can connect and enrich peoples’ lives—if done correctly and for the right reasons.

The 2017 Edelman Trust report, published recently, agreed that “we have a trust collapse”, adding, “We have moved beyond the point of trust being simply a key factor in product purchase or selection of employment opportunity; it is now the deciding factor in whether a society can function . . . the onus is on business to prove that it is possible to act in the interest of shareholders and society.”

A growing digital economy relies on trust. Breaking someone’s trust is like crumpling up a perfectly good piece of paper—you can work to smooth it over, but it’s never going to be the same. I have said it before and I will say it again: Managing information risk isn’t about saying “No,” it’s about protecting to enable people, data, and business. We have to run towards risk to shape the path of the risk curve. CISO’s need to do this, ideally, in front of business and technological opportunities or, at a minimum, in line with them. That is the best way we have to understand the risk dynamics to our organizations, shareholders, customers, and society. That is the best way to prevent risk that is avoidable in a proactive fashion.

If we carelessly implement technology in order to chase opportunities or simply prove that we can, we won't be successful in realizing digital transformations that can change lives and protect our people. Instead, we will be setting ourselves up for a digital disaster. By focusing on the opportunities along with our obligations to implement them right way, we can achieve digital transformation and digital safety to ensure tomorrow is better than today for everyone. With this mindset, we can avoid not only the digital free fall about which Myatt discussed, but also avoid the digital disaster that could lie ahead.

Conclusion

Thank you again for the opportunity to provide testimony. I will be happy to answer any questions.

The CHAIRMAN. Thank you, Mr. Harkins.
Mr. Rosenbach?

STATEMENT OF HON. ERIC ROSENBAACH, FORMER DOD CHIEF OF STAFF, FORMER ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY

Mr. ROSENBAACH. Good morning, Chairman Thune, Ranking Member Nelson, distinguished members of the Committee. Thank you very much for holding this important hearing, and thank you for the invitation. You've heard up until now from a lot of experts on the technology and the ecosystem in the United States, and I thought it might benefit the members of the Committee to hear the cyber perspective at a little bit of a more strategic level, based on some of my impressions in cyber issues in the last 7 years at the Department of Defense.

The rapid rise of emerging technologies and the Internet of Things will result in essential economic growth for America. This is important. The United States must continue to outperform competitor nations like China in the development and adoption of emerging technologies. These technologies must be a true economic center of gravity.

But as the number of Internet-connected, artificial intelligence-driven devices increases, policymakers and legislators need to address the associated increase in the nation's vulnerability to strategic cyber attacks. The fragility of our national cybersecurity posture combined with our adversaries' perception that Russia's recent successful cyber attacks on the United States will increase the likelihood that we will experience more serious attacks in the coming years.

As we unlock new technological innovation, we will live in a glass house that must be better protected, and without an improved defensive posture, this vulnerability may impact the calculus of U.S. national security policymakers down the road. Thus, it's important to understand the strategic perspectives of two competitors and sometimes adversaries in the cyber domain: China and Russia.

Over the past decade, China has pursued a national strategy to challenge the United States world leadership in emerging technologies. The Chinese government has invested heavily in research and development of technology that underpins supercomputing, artificial intelligence, and blockchain. Those investments have resulted in genuine achievements. Last year, for example, China unveiled the world's fastest supercomputer and announced that it owned more of the top 500 supercomputers than any other nation in the world.

Chinese firms and research institutions, nearly always supported by state funds, have made advances in artificial intelligence that some corporate leaders believe will make China the world leader in hardware-based AI within the next several years. Over the past 3 years, China has also strategically established itself as the world leader in the research and deployment of blockchain technologies, particularly in the area of financial technology, known as Fintech.

China currently leads the world in the number of citizens using Internet payment and Fintech applications, and the government continues to facilitate the growth of this sector with a permissive regulatory environment and strong investments in Fintech firms. China recognizes that the Fintech Revolution is about more than fancy payment apps and Bitcoin. It has the potential to disrupt the American-dominated financial sector and increase Chinese economic influence around the world.

Although the vast majority of Chinese investment and research in these emerging technologies focuses on improving the country's economic competitiveness, China also has programs dedicated to integrating new technology into security-focused cyber capabilities. For example, the Chinese have incorporated AI and supercomputing technology into the Great Firewall of China. These advances give China an upper hand not only in defending their domestic critical infrastructure, but also in taking offensive actions against key targets, including the United States.

Moving on to Russia, investment and research in emerging technologies are likely a decade behind the U.S. and China. However, President Putin has taken a deep personal interest in quickly closing this gap. In the meantime, Putin's recognition that his military does not have the ability to go head-to-head with U.S. next-generation military capability drives the Russian strategy to develop cyber capabilities to disrupt new technologies in both civilian and military environments.

In short, the Russians know that they can impact American strategic calculus—and control the escalation ladder of conflict—by attacking civilian targets in the Internet-of-Things and the military networks that connect AI-enabled weapons. Combined with the Russians' proven deep experience with spreading strategic disinformation, this form of cyber warfare should be a serious concern.

Russia's demonstrated willingness to conduct cyber attacks against civilian targets is unprecedented and has serious implications for a world that relies on the Internet-of-Things. Recent Russian cyber attacks against Ukraine took down a significant portion of that country's power grid and represented one of the first known cyber attacks that resulted in a physical effect. But these attacks barely drew criticism, let alone action, from the international community.

Additionally, every American should be deeply concerned that the United States democratic system of government was attacked by Russia during an important Presidential election. This is not a partisan matter. Our democratic system serves as an example to the free world. We must overcome politics and protect ourselves and allies from being undermined by adversaries in the future.

Without clear action in the near term, the Russians' inevitable perception will be that they can conduct strategic cyber attacks

with impunity. This will likely result in further attacks in the future.

Mr. Chairman, in the interest of time, I'll submit the rest of my statement for the record to allow you all to ask as many questions as possible.

[The prepared statement of Mr. Rosenbach follows:]

PREPARED STATEMENT OF HON. ERIC ROSENBACH, FORMER DOD CHIEF OF STAFF AND FORMER ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY

Chairman Thune, Ranking Member Nelson, and distinguished members of the Committee, thank you for calling this important hearing on "The Promises and Perils of Emerging Technologies for Cybersecurity" and for the invitation to testify today.

The rapid rise of emerging technologies and the internet-of-things will result in essential economic growth for America. This is important: the United States must continue to make the development and adoption of emerging technologies an economic center of gravity. But as the number of internet-connected, artificial intelligence (AI) driven devices increases, policymakers and legislators need to address the associated increase in the Nation's vulnerability to strategic cyberattacks. The fragility of our national cybersecurity posture, combined with our adversaries' perception that Russia's recent cyberattacks achieved unprecedented success, increases the likelihood that the United States will experience more serious attacks in the coming years.

As we unlock new technological innovation, we will live in a glass house that must be better protected. Without an improved defensive posture, this vulnerability may impact the calculus of U.S. national security policymakers. Thus, it's important to understand the strategic perspectives of two competitors and adversaries in the cyber domain: China and Russia.

Chinese and Russian Strategy for Emerging Technologies

Over the past decade, China has pursued a national strategy to challenge the United States world leadership in emerging technologies. The Chinese government has invested heavily in the research and development of technology that underpins supercomputing, artificial intelligence, and blockchain. Those investments have resulted in genuine achievements. Last year, for example, China unveiled the world's fastest supercomputer—and announced that it owned more of the top 500 supercomputers than any other nation in the world. Chinese firms and research institutions, nearly always supported with state funds, have made advances in artificial intelligence that some corporate leaders believe will make China the world leader in hardware-based AI.

Over the past three years, China has also strategically established itself as the world leader in the research and deployment of blockchain technologies, particularly in the area of financial technology (known as Fintech). China currently leads the world in the number of citizens using Internet payment and fintech applications, and the government continues to facilitate the growth of this sector with a permissive regulatory environment and strong investments fintech firms. China recognizes that the "Fintech Revolution" is about more than fancy payment apps and Bitcoin. It has the potential to disrupt the American-dominated financial sector and increase Chinese economic influence around the world.

Although the vast majority of China's investment and research in these emerging technologies focuses on improving the country's economic competitiveness, China also has programs dedicated to integrating new technology into security-focused cyber capabilities. For example, the Chinese have incorporated AI and supercomputing technology into the massive "Great Firewall of China" used to isolate Chinese Internet users from the outside world. These advances give China an upper hand in not only defending their domestic critical infrastructure networks, but also in taking offensive actions against key targets, including in the United States.

In Russia, investment and research in emerging technologies are likely a decade behind the U.S. and China; however, President Putin has taken a deep personal interest in quickly closing this gap. In the meantime, the clear recognition that Russia's military does not have the ability to go head-to-head with next-generation U.S. military capabilities has driven the Russian strategy to develop military cyber capabilities to disrupt new technologies in both civilian and military environments. In short, the Russians know that they can impact American strategic calculus—and

control the escalation ladder of conflict—by attacking civilian targets in the internet-of-things and the military networks that connect AI-enabled weapons. Combined with the Russians’ proven deep experience with spreading strategic disinformation, this form of cyberwar should be a serious concern.

Russia’s demonstrated willingness to conduct cyberattacks against civilian targets is unprecedented and has serious implications for a world that relies on the internet-of-things. Recent Russian cyberattacks against Ukraine, which took down significant portions of that country’s power grid and represented one of the first known cyberattacks that resulted in a physical effect, barely drew criticism—let alone action—from the international community. The Russians’ inevitable perception that they can conduct strategic cyberattacks with impunity is likely to encourage further attacks in the future.

Every American should be deeply concerned that the United States’ democratic system of governance was attacked by a foreign nation during an important presidential election. This is not a partisan matter. Our democratic system serves as an example to the free world. We must overcome politics to protect ourselves and our allies from being undermined by our adversaries in the future.

Chinese and Russian strategies for dealing with emerging technologies present the United States with two very different challenges: In China, the U.S. faces a competitor who is focused primarily on developing next-generation technologies more quickly than the U.S. in order to displace us as the world’s economic and military leader. In Russia, the U.S. faces an adversary who seeks to use advanced cyberattacks and information operations to undermine the strength of our democracy and the efficacy of next-generation military technologies.

Although the challenges posed by these nations differ, both cases underscore the need for a new national cybersecurity strategy that forces bold action and cooperation by the government and private sector. To mitigate the risk of cyberattacks, one essential component of this strategy should be for the government and private sector to invest in and adopt new technologies that will aid cyber defense, such as AI-enabled cybersecurity, cloud-based security-as-a-service solutions, blockchain and super/quantum computing. Facilitating the development of these technologies will not only improve our cybersecurity, but also strengthen one of the few remaining American economic centers of gravity.

Additionally, a new strategy for national cybersecurity cyberspace contains at least three other components: (1) the U.S. must immediately bolster deterrence of cyberattacks that threaten vital national interests; (2) Congress must clarify key regulatory issues that would promote the growth of key technologies with large potential to facilitate economic growth, such as blockchain and FinTech, and; (3) Congress must pass targeted legislation that provides the private sector with a framework for improved cybersecurity standards and incentives for information sharing.

The U.S. has enjoyed extraordinary economic success because of the open Internet we created—it is imperative we lead the world in securing it for decades to come.

The CHAIRMAN. Thank you, Mr. Rosenbach, and I’m going to yield my time in the interest of giving as many people an opportunity to ask questions to Senator Wicker.

**STATEMENT OF HON. ROGER F. WICKER,
U.S. SENATOR FROM MISSISSIPPI**

Senator WICKER. Well, let me just ask all of you to tell us what needs to happen in the workforce and in our American education system to meet these opportunities and challenges. And we might as well just start with Mr. Barlow and go down the line. Are we ready? Are we anywhere where we need to be?

Mr. BARLOW. Thank you, Senator. Well, as I stated earlier, we’ve got a 1.5 million person gap globally, and there are a couple of things we need to do. One of the things we’ve got to recognize is we need more women in this field. You know, the number of women in the cybersecurity space and technology in general is far too low. We also have to look at—

Senator WICKER. What is that figure here in the United States?

Mr. BARLOW. I don’t know, but I could get it to you in our comments. It’s very low, sir, particularly in the technical security

ranks. When we look for things like security operations professionals that would sit in an operation center, the number is very, very low.

But in addition to that, when we look toward universities, one of the things we really need to do is have universities step up and start producing degrees at scale. You know, the last time we saw an entrant in the C suite, it was the chief information officer. Well, now we have a chief information security officer. Where are the departments? Where are the degree programs?

But I think the last and most important thing is we've also got to look toward what we call at IBM new collar jobs, ways in which we can bring people in that maybe don't have a traditional 4-year degree in computer science and train them up to work in a security operations watch floor. And we think that that's absolutely possible when we augment those people with technology that can help bring them up to speed quicker and help them learn.

Senator WICKER. Where are we going to find these people? What level of education do they need to have before we bring them into training for new collar jobs?

Mr. BARLOW. Well, I think that, you know, one of the things we have to recognize is in the cybersecurity space, we need not only traditional technologists, but we also need people like linguists. So we're going to find them from all over. I think the real question is: Do they have the willingness to learn the forensics, learn the technological, and learn the science behind it?

What I find that I think is so fascinating is that the kind of mindset that you bring into a security operations center is much more analogous to what you might find in a traditional law enforcement career. You need people with an investigative brain, and I think we can find those people well beyond where we've traditionally looked for IT talent.

Senator WICKER. Others?

Mr. GANESAN. Thank you for the question, Senator. I actually think this is a tremendous opportunity for us. Yes, we have a shortage of cyber skills, but there's an opportunity to create a million-plus, maybe 2 million jobs in this country that are going to be high-paying, high-skilled, and cannot be outsourced. Because of various reasons, you want people doing cybersecurity to be based here.

I think the opportunity is: you don't need to go to college. You can, but you don't need to. You don't need a four-year degree. A two-year program, a one-year vocational program can get people good enough to do a lot of the security operations jobs we're talking about, and I think these can be skilled jobs that are high-paying, resident here, and I think if you put a collective focus on it, this will be both an offensive move in making sure we have the right cybersecurity infrastructure in this country and a move to re-energize our economy and create jobs in America.

Mr. GROBMAN. I would agree with many of the statements made that we do need to look to non-traditional methods to get people into the cyber workforce. One thing that's unique about cybersecurity as a profession is it rapidly changes, so the skills that you need today are not going to be the skills that you need tomorrow. The

typical individual in cybersecurity needs to be able to continuously learn and adapt to the ever-changing threat landscape.

Unlike a civil engineer who may use the principles of statistics and dynamics that will suit them well for their 40-year career, what you know about today will need to be completely retooled. So partnering with our government, looking at things such as the potential for a cyber national guard as well as really focusing on community colleges as well as traditional educational institutions are key things.

Mr. HARKINS. I would like to add some perspective to the 1.5 million job gap that we have. If you look at that—and, again, from a perspective of somebody who has run this—the reason why we have that gap is because we haven't prevented the problems. Most of those job openings are reactive—to detect and respond.

I think the bigger skill gap that we have is, again, how do you design and develop technology with less vulnerabilities to begin with? If you did that, we wouldn't have as big of a skill gap. If we had better technology that actually prevented the harm, we wouldn't have as big of a skill gap.

Now, I still think we're going to always need the fireman and the responders, and we're going to need the investigators, and I agree with the comments that we need people with a diverse set of backgrounds. But I also think we need to go earlier in the education cycle. We need to start at the grade school and high school level and teach basic skill and acumen, how to do coding and how to do it right, and then further that education when people get into undergraduate and postgraduate work.

Mr. ROSENBAUGH. I'll be very quick. We struggled with this problem at the Department of Defense when building Cyber Command and trying to protect all our networks. So there are two strategies, in brief. First, we decided to grow these individuals internally, which meant that we put them through high-end training. After a year and a half, they would have pretty high-end skills, the equivalent of a Special Forces operator in the cyber world.

Now, we want them to stay in the military, but if they decide to get out, that's a great pipeline for that highly skilled workforce that benefits the rest of the economy. You see that model very pervasive in a lot of other countries, Israel in particular.

Second, we've worked very closely with the National Guard to have citizen soldiers that will go in and out of the military, develop skills, but then also take those skills back to the private sector. Building on those two models is something that I think holds promise.

Senator WICKER. Thank you.

The CHAIRMAN. Thank you, Senator Wicker.

Senator Nelson?

Senator NELSON. Yesterday, the Director of the FBI outlined what the Russians had done in this past election, and he opined they may be planning to do it to us again in 2020 and possibly 2018. Just 4 days ago, four Russian citizens were indicted in a scheme that took 500 million accounts from Yahoo. So they now have the capability of spying on White House officials, military officers, bank executives, and airlines. So the actors, Russia and China—this, of course, is pretty serious business.

So what, really, Mr. Rosenbach—if they can get access to the personal, financial, and health information, then they really have the keys to being able to manipulate citizens as well as the government. So why is the country not alarmed?

Mr. ROSENBACH. Senator, I don't know as much about why there's not more alarm about this. To me, personally, this is something that is very, very serious. And, as you heard from my opening statement, I think deterrence is a very important aspect of this. Deterrence is something that is an inherently governmental role, and we need to think about how to bolster our deterrence posture so that not only the Russians, but other adversary states do not have the perception—because deterrence is based in perception—that they can influence the American democratic system for either way, and I don't mean this in any partisan manner, but that is a core national interest, defending our democracy.

Senator NELSON. Do you think the structure that we have now, which we passed, but it's voluntary—a cybersecurity bill—it's voluntary. Do you think voluntary cybersecurity efforts in the private sector are going to meet this challenge?

Mr. ROSENBACH. Sir, I don't. I believe that the framework that NIST put together, which uses public-private collaboration, is very strong and is important and is something that should be in legislation. I also believe that there should be a system of incentives for increased threat information sharing, as you heard one of the earlier witnesses talk about, and that there's some liability protection put in place for that. Otherwise, I don't think there's a mechanism that will influence things to change.

Senator NELSON. So you don't think that these are just private cyber intrusions? These are threats to national security.

Mr. ROSENBACH. Yes, sir, absolutely. As you saw from the DOJ action, these were both FSB-affiliated individuals, FSB agents, and then people affiliated with FSB, probably from some criminal organization. The nexus between those two is tight. That's the standard MO for the Russians.

Senator NELSON. And what they have been doing is changing or manipulating data to influence public discourse, in this case, in the election, and to create confusion. So, obviously, Russia took advantage of this. Do you think that these technologies can help us, our country, defend from future election tampering?

Mr. ROSENBACH. Yes, sir, I do, and you could ask some of the folks who are deeper into the technology. But, for example, the idea behind blockchain, that there would be a ledger in which you cannot manipulate the outcome of things, is attractive when it comes to election and perhaps electronic voting. However, I would say that technology is very, very important. There's a lot more to this than just the technology.

Senator NELSON. Any comment from—Mr. Grobman?

Mr. GROBMAN. Senator, the one thing I would add, which was in your opening remarks, is one of the big shifts that we see right now is cybersecurity is moving away from just being about theft of data and data being used as a weapon itself. Using the data to extort or cause harm is one of the things that we've not only seen in the election cycle, but that is the same type of damage that is done through the Yahoo attack. So it's important when we think about

cybersecurity that we're thinking about it broadly in terms of many areas, especially in this emerging field of using data as a weapon.

Senator NELSON. How would you defend if someone put child pornography onto someone's data system, their laptop, and then tipped the police that this person is a child pornographer? How would you defend against that?

Mr. GROBMAN. I think one of the biggest risks that we have today is the general public treating leaked data as having integrity. One of the big challenges is especially around intermixing legitimate data with fabricated data. You can increase the confidence that data is real by having part of that data be accurate, that can be independently verified, but then overlaid with fabricated data. Whether that fabricated data is included to cause political harm or to falsely indict someone in a criminal case, it is critical that we treat any leaked data with suspicion until every element of it is independently validated.

Senator NELSON. Thank you.

The CHAIRMAN. Thank you, Senator Nelson.

Senator Cantwell and then Senator Inhofe.

**STATEMENT OF HON. MARIA CANTWELL,
U.S. SENATOR FROM WASHINGTON**

Senator CANTWELL. Thank you, Mr. Chairman, and continuing along this same line, I wanted to make a point that I'm glad to hear this 2 million job number. The Energy Committee has already been on this task, and we definitely passed a very good bill out of the United States Senate that was all about the various elements that we need to do on workforce; information sharing; supply chain security, which we haven't spent a lot of time talking about this morning thus far; and R&D.

Unfortunately, our House colleagues just did not get the urgency of this. So if any of my colleagues here can help us with our House colleagues—I mean, literally, in negotiations and conference, they didn't even—I mean, they almost looked at it as like some sort of political issue on our side or something. I don't know. It was just very, very disappointing that they did not see the urgency of this issue.

The reason I bring that up—and I do want to allude to the earlier comments by Mr. Barlow and Mr. Ganesan—the University of Washington Tacoma, which happens to be also the area of Joint Base Lewis-McChord, our National Guard—so there's a lot of defense and education overlap on security, so they're working very well.

But they do have a master's of cybersecurity and leadership. They have a bachelor's of engineering and cybersecurity, and then a two-year certificate in cybersecurity operations. So we've definitely heard—I would throw on an education person, too, that we need the educators to educate the people. So they've already identified at that school these various workforce issues, and, as I said, DOE in our energy bill was supposed to add to those workforce requirements.

But back to this issue of the grid and Russia, because what we've identified, too, is we want DOE to be a lead role on critical infrastructure because the issues that we all just discussed here require

DOE and the grid to be modernized and continue to have that security discussion with various providers.

So I don't know if we start with you, Mr. Rosenbach, but the Ukrainian attacks, Kiev, are something that we could very easily see here in the United States by a government actor, if not Russia, others. Is that correct?

Mr. ROSENBAACH. Yes, ma'am, absolutely. The malware that was used in the Ukraine attack was actually a variant of something that we've seen on the networks of critical infrastructure operators in the United States—so-called black energy—even in power grids. So it's not just a theoretic case that it could happen. It could happen, and in the case of the United States, because the critical infrastructure networks are so much more highly automated, the damage could be even more severe. In Ukraine, they were able to manually bring things back up.

Senator CANTWELL. Right. I've heard people discuss the possibility of a cyber 9/11, which I'm assuming they're referring to the context of a great-scale disruption and chaos. But in some cases on this critical infrastructure, they've talked about the disruption that such malware could do to an actual natural gas or oil pipeline or other critical energy infrastructure.

I always find it interesting when you see these movies, like *Black Hat* or what-have-you, it's always connected to energy. It's always connected to disrupting energy supply as a way to also send a shockwave—I don't know if either of the other witnesses want to comment on the security of that and how important it is to have DOE play a role on the critical infrastructure development.

Mr. HARKINS. Senator, I think it is absolutely critical, and I think you're right, and I think that critical infrastructure, as it was mentioned, does have risks. But, again, going back to the context of where we're thinking about emerging technologies and Internet of Things, let's just say we hardened the electrical grid and hardened the traditional critical infrastructure. The same effect could occur if I attacked my home that's fully automated, and take out my heating, air conditioning, take out the smart meter on my house that's connected to the Internet. And if you do that en masse across a metropolitan area, you could keep the grid up, but if you still affected, let's say, a million people in the greater Phoenix area during a 120-degree heat wave because you're able to shut off the refrigerator, shut off their air conditioning, shut off the electricity in their house, you could have the same effect.

Senator CANTWELL. You're making my point for me.

Mr. HARKINS. Yes.

Mr. GANESAN. If I could add, Senator?

Senator CANTWELL. Thank you.

Mr. GANESAN. I think critical infrastructure is—I mean that broadly, as in dams, power grids, electrical grids. That is a big area of vulnerability for us, and I actually don't think we are fully prepared. I think what Stuxnet showed—that you could have access to these—what they call PLCs and static control systems that are not connected to the Internet, and once you're in, you could impact them. And I do think we need to think about both standards and evolution there.

In addition to that, you mentioned something equally important, supply chain security. If you think about it and look at some of the major hacks, those hacks came in because the vendors were compromised. So I think we need to have a better way of knowing the supply chain, if people have access to a network, and making sure the entire supply chain is secure because in cybersecurity, you're only as strong as your weakest link.

Senator CANTWELL. Exactly. That's why we want this DOE upgrade, and to make sure that we do that. And then to Mr. Barlow's point, having this larger discussion, which is very hard to have, you know, necessarily, with our utilities and some of our other critical infrastructure with the R&D side. People don't want to talk about their vulnerabilities, but yet we need to get best practices out there based on the latest and most significant risks.

Mr. BARLOW. I think this raises a really key point, in that part of what I would encourage you to go back and really think about is speed. You know, whether we're talking about black energy, whether we're talking about other forms of attacks—I mean, you know, if we look right now at what's going on in Saudi Arabia and the Gulf states as they respond to Shamoon and Shamoon 2, which is affecting the petroleum and chemical industries, you know, these are, in many cases, significant attacks that have a kinetic outcome in terms of their impact on business, or they may stop various manufacturing lines.

At the end of the day, what actually makes the difference is the speed at which the private sector and the public sector, across multiple governments in many cases, work together. And by having that threat intelligence with speed—now, think about what that requires. That requires not only the culture and the ecosystem to move fast, having an on-mission culture across the board, but it also requires having the security clearances in place for people to have those dialogs at an operational level, and it requires the clearinghouse in order to manage those vulnerabilities.

The CHAIRMAN. Thank you, Senator Cantwell.
Senator Inhofe?

**STATEMENT OF HON. JIM INHOFE,
U.S. SENATOR FROM OKLAHOMA**

Senator INHOFE. Thank you, Mr. Chairman.

At the risk of sounding redundant, which I will, for the benefit of the witnesses, there are two very significant committees, the Commerce Committee and the Environment and Public Works Committee. There are nine committee members on both committees, and we always have our meetings at the same time. So the disadvantage is you get—you miss all—I would miss, in this case, all of the opening statements and what questions have already been asked. So that's one of the problems that we're going to try to get the leadership of both committees together to try to rectify since we deal with very similar subjects.

Let me go ahead and just cover some of the—it may have been covered. Stop me if it has been.

Mr. Grobman, cybersecurity is enhanced when products are built from the ground up protected from cyber attack instead of trying to impose cybersecurity protections after the product has been de-

veloped. I think we understand that. Unfortunately, there are not always strong market incentives for companies to build products from the ground up with a focus on cybersecurity, which has encouraged sentiment for hard regulations to force the integration of cybersecurity into the development of consumer products.

So, first of all, do you agree that is a problem? And can you speak to the harm that structured hard regulations would have on cybersecurity innovation?

Mr. GROBMAN. Absolutely. To the first point, one of the big challenges that we see is sometimes the attack on a device isn't going to harm the individual that purchased the device. In the case of the Mirai attack back in October, although a consumer purchased a DVR, they weren't the ones harmed when that DVR turned and attacked Dyn and then provided denial of service against Spotify and Twitter. So there would be a natural sentiment to look for ways to regulate the way you build those devices.

One of the challenges that we see with hard regulation in cybersecurity is, given that the threat landscape continuously changes, being overly prescriptive on how to build a device can make it so that companies are focused on being compliant and removing opportunity costs they would otherwise apply to addressing the most critical threats of the day, making their device less secure.

Our recommendation is to focus more on a framework very similar to what we've done with the NIST framework that can provide a blueprint for manufacturers to ensure they're looking at the key areas, but be flexible enough so that it's constantly tracking the latest threats of the day, and that the manufacturers and organizations always have the ability to focus on the most profound threats versus specific elements that are imposed in a regulation.

Senator INHOFE. So what you're pointing out is that, yes, it is true that if you have to do this—but if you do it to that detail, they'll forget what the real purpose is, whether it's safety or other elements. Do the rest of you agree with that kind of a—

Mr. GANESAN. If I could add, Senator, I completely agree with Mr. Grobman. Because cybersecurity is so dynamic, if you try to do hard regulations, it's sort of like closing the barn door after the horse has bolted, because you're fighting the last war instead of the next war. So I think it's much better to have guidelines and visibility and flexibility and let the market forces determine—

Senator INHOFE. That makes sense. That does. That's a good comment.

Some of you talked about the value of the public and private partnership. Usually, you're talking about government and industry. However, as was brought up by Senator Cantwell, the universities are getting involved now, and it happens to be that the University of Tulsa—and I assume some of you are aware of this—has won the Southwest Regional Collegiate Cyber Defense Competition for the second year in a row. Any comments you would make about the inclusion of programs like that one that has been very successful in Tulsa University?

Yes, sir?

Mr. BARLOW. Well, I was very disappointed to see their win because they won against my alma mater, Rochester Institute of Technology.

[Laughter.]

Mr. BARLOW. But that aside, you know, all kidding aside, I think it's really exciting to see these kinds of competitions, and——

Senator INHOFE. I think so, too.

Mr. BARLOW. Well, you know, because part of what we have to all understand in this, right, is that in order to be good defenders, we have to understand how offense works. We have to understand both sides of the game, and this is a great way to give students the opportunity to learn, to do something a little bit different. And, interestingly enough, we're trying now to take this, frankly, to adults as well, which is why IBM has built the Cyber Range in Cambridge, Massachusetts, to give people the opportunity to practice and rehearse not just the technical side of this, but how to deal with regulators, how to deal with unhappy customers, how to deal with the press and media post-breach. I mean, I would argue that in many, if not most, breaches we see, the response to the breach often causes more damage than the breach did itself.

Senator INHOFE. And you would agree that you are actually, in this program, leading some of these young people into that career.

Mr. BARLOW. Absolutely. This is actually one of the reasons why we have been active sponsors of these types of university competitions.

Senator INHOFE. Yes, and we appreciate it.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Inhofe.

Senator Schatz?

**STATEMENT OF HON. BRIAN SCHATZ,
U.S. SENATOR FROM HAWAII**

Senator SCHATZ. Thank you, Mr. Chairman.

I want to follow up on the question asked and the sort of, I think, consensus view of the panel that if we try to lock in a regulation, either through rule or statute, that the technology will just outrun it, and I'll stipulate to that.

But the question I have is if NIST is our framework, the real challenge is we don't know what the adoption rate is in the private sector. I'd like, if you wouldn't mind, just a quick yes or no and maybe a few comments on whether or not each of the panelists think it would be in the public interest for NIST to collect data on adoption rates so we know whether or not this NIST framework, private sector-driven, innovative, nimble, is being adopted, because all of that makes theoretical sense, but if it's not being adopted, or we don't even know the adoption rates, then we're working in the dark.

It seems to me that all of you are data people, so you might be amenable to the idea that we should know what private sector actors are doing here.

Mr. Barlow, to start.

Mr. BARLOW. Well, I think it's an excellent question, Senator, and we've actually studied it, and we'd be happy to provide you with the details of that study, where we didn't look specifically at

just the NIST framework. We looked at frameworks overall, because I think one of the things that the NIST framework excelled at was giving people a guideline and allowing them to customize it.

Senator SCHATZ. But the question is do you think that we should be collecting data on the percentage of companies in the private sector that are adopting the NIST framework?

Mr. BARLOW. I think you need to ask the question a little differently, in my opinion, which is how many companies have a framework that they're following? I think it's OK if they use it as a guideline and tweak and tune it based on industry or based on what their particular threats are. But what is absolutely critical is that private sector companies and governments have a framework that they're following so that they have both breadth and depth across all—

Senator SCHATZ. Whether it's NIST or some other framework—

Mr. BARLOW. Exactly. COBIT, whatever.

Senator SCHATZ. Fine. But we need to know where we're at, and it seems to me that we're operating in the dark as policymakers here. We'll just go down the line as quickly as possible.

Mr. HARKINS. Senator, I totally agree with you. I think the collection of that data is useful, and I also agree with Mr. Barlow that there are multiple frameworks. We need to think about which ones. And just having a framework by and of itself doesn't mean that you're actually applying the framework appropriately. So it would be like giving somebody a calculator and saying, "Are you using the calculator?" It doesn't mean they're doing the calculation correctly.

Senator SCHATZ. No, but we know they're not doing the calculation correctly if they don't possess a calculator. Right?

Mr. HARKINS. I absolutely agree, yes.

Mr. GANESAN. I like market forces, Senator, and so one of the reasons why I've been pushing cyber insurance is now you have a market force for people to get cyber insurance. The insurance companies will need to underwrite, and one of the questions they will ask when they're underwriting is, "Are you following the NIST framework?" And your premiums will be based on how well you follow this.

So market forces which actually have money at risk will drive people's behavior than regulatory purposes, because what that becomes is compliance, as opposed to having a market dynamic that feeds into what you do.

Senator SCHATZ. As quickly as possible, please. Thank you.

Mr. GROBMAN. I agree with Mr. Barlow. I think the challenge with assuming NIST is the only framework is NIST is a great solution when customers are looking to improve their cybersecurity posture. It's something that, very often, if I go to a customer, and they ask, "Do you recommend a framework?," I will point them to NIST. But for other organizations that have been operating for many years using another methodology, I would not hold them at fault for that. So I think studying it is good, but I don't think one size fits all.

Senator SCHATZ. Right. But we should be collecting data.

Mr. Rosenbach, I want to ask you a different question. One of the policy recommendations from the panel has been to revise the proc-

ess that the administration uses to determine whether to disclose a vulnerability to a vendor or to retain it for national security purposes. Senator Johnson and I are working on a bill that would improve and codify the process. Can you tell us why you think this process is important to codify and why it's useful to business?

Mr. ROSENBACH. Yes, sir. I do think the process is important. So I'll state up front there are cases in which the government needs to keep zero-day vulnerabilities to ourselves for national security reasons. I'll caveat that by saying if we can't keep those secret, and there are going to be a lot of insider disclosures as there have been, then we undermine our credibility for saying that we can't disclose vulnerabilities.

Second of all, in the Department of Defense, Secretary Carter took very, very seriously the need to rebuild bridges with Silicon Valley after the Snowden disclosures, and part of that is transparency. And if we know that the greater good is disclosing some vulnerabilities to vendors and firms that are U.S. firms, that's good for the country, because we want it to be the center of gravity for the economy, and if we don't do that, we're kind of shooting ourselves in the foot.

Senator SCHATZ. Mr. Grobman?

Mr. GROBMAN. I think the key thing is transparency, because what we do need to recognize is some vulnerabilities the government is aware of will make sense to keep private, and others will be in the greater good to use responsible disclosure and get addressed. We need to look at things such as what is the probability it will be independently found by other adversaries. There are many elements that need to go into that decision, and being transparent on the criteria is a great way to be open about what it is we're doing while keeping the classified information classified.

Senator SCHATZ. Thank you.

The CHAIRMAN. Thank you, Senator Schatz.

Senator Markey?

**STATEMENT OF HON. EDWARD MARKEY,
U.S. SENATOR FROM MASSACHUSETTS**

Senator MARKEY. Thank you, Mr. Chairman.

Mr. Rosenbach, I'm working on a piece of legislation right now that I'm going to call Cyber Shield, and it's with this idea—because of the spread of the Internet of Things, whether it be an automobile, a toaster, you name it, they're all going to be vulnerable to hacking. Right now, the American public doesn't know how vulnerable they may be.

So on cars, we've got—here's your fuel economy sticker, here's the safety of the car sticker, and so people can make a judgment. So what would you think about that idea, that on a voluntary basis, but here it is, like kind of Energy Star—it's on the car, it's on the toaster, and it gives you kind of a one-star through five-star rating as to the level of cybersecurity that has been built into that device? That would incentivize companies to kind of meet the higher standard as people get more concerned about it.

What would you think about that as an idea?

Mr. ROSENBACH. Yes, sir. I'm a huge fan of creative ideas that allow people to understand the problem and facilitate the flow of

information about cybersecurity, so I think that sounds good. In particular, if it's worked in conjunction with the private sector so that everyone understands how the evaluation would work, it seems like a good idea.

Senator MARKEY. What do you think about that, Mr. Harkins?

Mr. HARKINS. You know, I think it's a great idea, and I was smiling when you were saying that, because a few years ago when I was at Intel as Chief Security and Privacy Officer, we had floated the idea of creating a security star rating. It's an interesting concept and I think one that has merit.

I think it can be practically hard to implement, though, because it would be like the miles per gallon. Because the technology is evolving, there might be a deterioration of the rating, and so how do you keep that up to date.

Senator MARKEY. I appreciate that. We'd have to figure it out, but—

Mr. HARKINS. Yes, we would.

Senator MARKEY.—the public has a right to know as well.

Mr. HARKINS. Absolutely.

Senator MARKEY. Do you agree with that, Mr. Grobman?

Mr. GROBMAN. Senator, I would note a tone of caution. I think that there is a risk in that sort of approach, in that even devices that were built with high levels of quality in their security architecture are still subject to having vulnerabilities in the future, and if having the five-star rating on a device at the time of manufacture gives the user of that device the thought that it is going to be good, I think it can lead to issues—

Senator MARKEY. Assuming that we could do it with that caveat, that, you know, over time it could erode, but just so—it's a 2014, here's the standard for that.

Mr. GROBMAN. I just don't know if the general public is able to comprehend that level of intellect that even if they had a five-star rating when they bought the device, it still may become vulnerable in the future.

Senator MARKEY. One of the criteria would be whether or not the technology has an ability to alter to changing threats, too. That could also be up there, so that the public could understand that.

Let me go to you, Mr. Ganesan.

Mr. GANESAN. Senator, I find this nuance because I always think of the perspective of the small entrepreneur. That's the companies we back, and a lot of well-intentioned government regulations end up putting a lot more burden on small companies and their ability to innovate, because those companies don't have expensive lawyers and they don't have—

Senator MARKEY. This would just be voluntary.

Mr. GANESAN. So I understand, Senator, and I would say that I find that market-driven initiatives are better than government regulations.

Senator MARKEY. Right. But if there is no—right now, there's nothing, so the market's had years to do something and they don't do anything. So in the substitution for that, you introduce something that's voluntary, so that would be my point.

Mr. Barlow, quickly, please?

Mr. BARLOW. So I think at the end of the day, what you need to do is hold manufacturers responsible for a few key things. When products ship, they need to ship not with default user IDs and passwords. We need to understand how the data that these devices collect—how it's being used, where it's being stored, what the security posture is around it.

And we also have to recognize that these devices—I mean, how old is your computer, sir? It's probably only a year or two old, right? I mean, I've got a 10-year-old car. We've got to have the ability to update things. The thermostat that goes in your house might be there for 20 years.

Senator MARKEY. I got it. I just have one more question. I just will say this is actually going to give small companies a chance to stand out and say, you know, we've got this new device so you can—not only—we're selling it, and the small companies could kind of just move it. So that would be a great venture capital entrepreneurial opportunity.

Finally, on the question of cybersecurity vulnerabilities directed to the—you know, in the airlines. It's a huge issue now. We're reading more and more about it.

Mr. Rosenbach, do you agree that the airline industry should share information about cybersecurity threats, attacks, and protections to the FAA and to other airlines when they're identified?

Mr. ROSENBAACH. Yes, sir. In principle, more information sharing is better. Whether you want the FAA to be the nexus, I think you should work with the private sector to make sure that they're up and able to do all that. But there are threats to the airlines, and it's very important to try to find some way to address those.

Senator MARKEY. And do you also agree that the FAA should establish cybersecurity framework for aircraft and ground support equipment?

Mr. ROSENBAACH. They should, as long as they do that with the private sector, too, so that it's within the technology that they work with.

Senator MARKEY. And that's the Cyber Air Act that Senator Blumenthal and I have introduced so that we can figure out what that framework should be so that information gets shared. If there's a cyberattack on United, American should learn about it, the FAA should learn about it, so all the vulnerabilities that might be identical would be shut down.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Markey.

Next up is Senator Peters.

STATEMENT OF HON. GARY PETERS, U.S. SENATOR FROM MICHIGAN

Senator PETERS. Thank you, Mr. Chairman, and thank you to each of the panelists. This is a fascinating discussion.

I want to focus on an area that I have been doing a great deal of work on, and actually working with Chairman Thune on, and that is automated vehicles. We've talked about, generally, some frameworks in looking at these kinds of products.

But, obviously, this is a piece of critical infrastructure. These vehicles will be highly connected. They'll not only be talking to each

other. They're going to be talking to the roadbed and will be in complete control, and it's much different if there's a cyberattack on an automobile than your bank account. We're all mad when our bank account is attacked and some money is stolen, but this could be existential if they take over your automobile.

I know the auto companies are focused on this a great deal. But I want to kind of get your assessment as to what you are seeing, if you've been working with them, and what you are seeing in terms of the work that they are doing. I know that 2 years ago, the auto industry and NHTSA developed an Auto ISAC, which, from my understanding, is working well. It's successful. It has now been expanded to suppliers as well, understanding that in order to get consumer acceptance for this product, you're also going to have to make sure that they are fully protected.

Mr. Ganesan, I believe you have some familiarity with this area. Do you think the auto industry is taking the right steps with that ISAC, and what role do you see in data sharing in connected vehicles among a variety of companies?

Mr. GANESAN. That's a very important question, Senator. I do wish to state for the record that we're investors in Uber which is developing self-driving cars, and so we do have an interest in this.

But I think that, yes, some progress has been made. I would actually say more progress needs to be made because, in essence, cars actually end up having a much longer timeframe. You keep them for longer and so, in essence, you need to have a way of updating them post facto. And the very fact that you need to update them also means there's a security risk, because if you can update them, so can the bad folks. I think that while progress has been made in terms of getting together, I think more needs to be done, and I do agree that having someone taking over an unmanned vehicle poses a much bigger risk, and I would say that more work needs to be done.

Senator PETERS. Although updating, as you said, is problematic, and the fact that you should try to design these right from the get-go to be secure—obviously, you need some updates—but it is a problem, as was mentioned by Mr. Barlow and others, when you have older vehicles out there as well that may have some interfaces with vehicles. So that's a challenge we've still got to deal with.

Mr. Barlow?

Mr. BARLOW. Well, you know, I think one of the fascinating things about the auto industry is this is a good proxy as we look across many other industries, whether we're talking about airlines or vessels at sea, of the types of things we need to consider. But we also have to consider not just the vehicle and the kind of kinetic actions that may occur, but what's happening to that data that's coming off those cars. Where is it being stored in the cloud?

You know, our X-Force threat researchers recently disclosed that we were able to identify multiple vehicles that once you sold them, you were still connected to them. So someone buys a used car, and the old owner is still connected to the vehicle. They can find out where it is. They can unlock it and in some cases could even drive off with the vehicle. You know, there's a good example of working with industry to obviously get this fixed, but it's a good example

of new challenges and new thoughts that we have to take into account.

What I would encourage you to think about is this isn't limited to what happens in the vehicle. It's just as important to think about what's happening in the cloud. A good proxy for this that gets even more interesting is when you start looking at vessels at sea. A cruise ship is a floating data center with all kinds of information and IoT devices on it, and we've really got to think about all the aspects of how that is managed.

Senator PETERS. Mr. Grobman?

Mr. GROBMAN. So the one thing that I would like to add is we really do need to think about autonomous vehicles as being new platforms. It's not that we're taking the cars of today and making them self-driving. It's one of the reasons that we are sponsoring a new organization, the Future of Automotive Security Research, to partner with the industry to figure out what are the new building blocks that are needed, everything from what is the right architecture for field upgrade ability, because we recognize if you're going to have a car in field for 10 years, you're going to need ways to remotely update it as well as have secure communications across the board.

The one other point that I think is critical is to recognize that the general public looks in aggregate at the risk that autonomous driving can lower as it relates to death in automotive cases, where we see autonomous driving as being much safer than human driving in the long run, and based on studies, we see things such as 95 percent of accidents are caused by human failure, not machine failure. So we need to look at that element as much as the new risk related to the cyber elements.

Senator PETERS. My time has expired. Thank you.

The CHAIRMAN. Thank you, Senator Peters.

Next up is Senator Cortez Masto.

**STATEMENT OF HON. CATHERINE CORTEZ MASTO,
U.S. SENATOR FROM NEVADA**

Senator CORTEZ MASTO. Thank you, Mr. Chair.

Thank you, gentlemen, for being here. I appreciate the conversation. I was the Attorney General of Nevada for years. This was an important issue for me to address and I still look forward to working with all of you in this space. One of the things—there are a number of topics. I'm going to try to get through them very quickly with your help.

Small businesses, in general. I was just home in Nevada, and one of the questions I repeatedly get from our small businesses is this is a space that they want to address and try to protect against, but, as you can imagine, there are concerns about resources, the ability, and then just understanding cybersecurity, in general, and being able to implement it.

Can you address a way that we can help to work with our small businesses to give them the opportunities that they need to protect against cyberattacks? And I'll open it up to anyone who would like to comment.

Mr. HARKINS. Senator, I think you're right, and I think small business has a challenge just like consumers have a challenge. I've

long thought that there's a security poverty line that exists, like a societal poverty line, and those that have the resources, the skills, the technical competencies to deal with these issues and those that don't. And I think in many cases small business is well below that poverty line, just like we see a lot of large businesses below that poverty line.

I think the only way we can get them to essentially punch above their weight limit and do better is to get them better technology that preempts the execution of malicious code and stops the bad things from occurring that can harm their business and harm their customers.

Senator CORTEZ MASTO. So that goes back to your security in the design and architecture, correct?

Mr. HARKINS. Not only in the design, development, and the implementation, but post-implementation. Any device that executes code has the potential to execute malicious code. We have to look at that code execution prior to it happening and determine good from bad. We've proven it can happen in milliseconds, and we've proven we can preempt the execution of malicious code.

Senator CORTEZ MASTO. OK. Mr. Grobman?

Mr. GROBMAN. One of the big advances that we're focused on along with the rest of the industry right now is shifting the way that we build cybersecurity defense solutions for cloud-based offerings, and one of the reasons that that is key to small business is what the cloud does is it abstracts the complexity to the organizations that are running the cloud implementation, whereas you don't need the same level of expertise within the small business that you traditionally did.

So one of the things that I would strongly advocate for the industry is to continue to move down that trajectory, but make sure that we're designing our systems with a wide enough dynamic range that they scale not only to large businesses and organizations, but also to the very small businesses as well.

Senator CORTEZ MASTO. Thank you.

Mr. GANESAN. I'll be brief, Senator. I think the easiest way is to make sure that capital formation and the ease of capital is easily available for entrepreneurs, because I think the way you bring down the cost for small businesses in terms of cybersecurity is by having more innovators focus on the market and making capital formation easier is a key to that.

Senator CORTEZ MASTO. Thank you. And then the topic on the skills gap, which clearly is an issue for the future. We are in the age of technology. It's going to continue to evolve, and we need to do a better job really training and preparing the workforce for the future.

I am proud that in Nevada, for the first time, our Governor's Economic Development Agency partnered with the private sector and our system of higher education, so we're working together. Let me give you an example. We went out and were able to incentivize Tesla to come to Nevada. Part of that arrangement was also partnering with the private sector as well as our system of higher education to develop the curriculum that Tesla will need for that skilled workforce. So we put them all in a room and work together.

I think that's how it should happen all the time. But that's not necessarily the case in every community.

I'm curious—and I'll open this up again—how we here at the Federal level can incentivize that type of coordination to ensure we are focusing on that skills gap and the curriculum that's necessary.

Mr. BARLOW. So I think there are a couple of key things that we can do, Senator. And, by the way, just to answer an earlier question on the percentage of women in the cybersecurity workforce—I was able to find that while we were talking—it's 10 percent today. There's a great example of a real opportunity, right?

But if we look at the things government can do, certainly incentives for universities to start to develop programs, and I don't just mean kind of a couple of classes—full-on cybersecurity programs. In addition to that, really looking at the transition from veterans into the security workforce. Not that any of us want to steal people out of the government, but when people are ready to retire from their time in government, there's an excellent opportunity for that transition. So I think those are two really simple things we can do.

But the other thing we can really look at is how can government, working with the private sector, help to influence these new collar job opportunities, where we're finding people above and beyond just people that pursued a traditional computer science degree, to bring them into this space and help solve the problem.

Senator CORTEZ MASTO. Thank you. I know my time is up. And one final thing I'm just going to throw out there, and we'll follow up on—I'm also concerned about patchwork regulation and legislation. We see the states—Nevada has done it. We had concerns, and so we developed legislation at the state level, then the Federal level coming in. There needs to be the ability, I think, to coordinate so we aren't stifling entrepreneurship, so we are working together to share information when it comes to that, the cybersecurity threat. So I'm just throwing that out there and would love to follow up with you to get your thoughts on that as well.

Thank you, Mr. Chair. I appreciate the opportunity.

The CHAIRMAN. Thank you, Senator Cortez Masto.
Senator Udall?

**STATEMENT OF HON. TOM UDALL,
U.S. SENATOR FROM NEW MEXICO**

Senator UDALL. Thank you very much, Chairman Thune.

This has been an excellent panel here today. Thank you for all your testimony.

In this committee, we have a bipartisan track record of promoting innovations and new technologies, but we cannot ignore that our new reliance on Internet-connected technologies can make us more vulnerable to cyber-attacks. So it's important that we explore ways to ensure basic consumer protections and cyber hygiene for new technologies.

Cyber threats are more than individual identity theft, stolen credit card information, or other cybercrimes. We also face cyber terrorism threats to our electric grid, to pipelines, and other critical infrastructure, and, most dramatically, the U.S. intelligence community is stating in no uncertain terms that we face threats from state-directed actors seeking to influence and undermine our elec-

tion process by manipulating social and online media. In our modern capitalistic economy, all of the important private sector firms in front of us today, play a role in defending America and our freedom, not just from cybercrime, but from cyber war.

Mr. Rosenbach, your testimony discusses how Russia has become increasingly emboldened in its use of cyber-attacks. You cite a lack of forceful response following cyber-attacks against Ukraine that took down portions of the power grid. Could you share more about the relationship between Russian cybercrime organizations and Russian intelligence operations?

Mr. ROSENBAACH. Yes, sir. There's a long history of the Russian intelligence services cooperating with Russian organized crime in order to carry out things that are within the Russian national interest. So you saw that clearly in the evidence behind the DOJ Yahoo case, but you see that in many other ways, too, but in cyber, in particular, because there will be members of the FSB or the GRU that also make money on the side or are part of those criminal organizations. So it makes it complicated, but it also makes it very important that the government understands that and have some type of response to it.

Senator UDALL. Thank you. The Federal Government spends—and I'm changing over to a new topic here, on legacy IT. The Federal Government spends \$80 billion annually on major IT systems. The bulk of that money goes to maintaining and operating legacy IT. GAO has noted that legacy IT systems result in higher costs and create security vulnerabilities. Some tech companies have sold IT that is still being used by Federal customers, even though the product is no longer supported. That means no customer support, no automatic software updates with security patches, for example.

Mr. Grobman and Mr. Barlow, is it a good idea for Federal agencies to use vulnerable IT products that are no longer supported by the manufacturer? And do you agree that it makes sense to replace outdated IT systems when they create cyber risks and when a new technology is more cost effective?

Mr. GROBMAN. It's absolutely critical to rapidly move to new, modern technologies, not only for the reason you cite, that older technologies have vulnerabilities that could be exploited by bad actors, but also the technology itself. The new, modern systems they are built on are inherently more secure than being able to retrofit or try to defend those legacy systems.

So think of it in terms of our physical infrastructure. Occasionally, we'll have an old bridge. We can do a retrofit to it in order to make it seismically stable. But sometimes there's no alternative but to build a new bridge, and that's the same mindset that we need to think about as we triage the systems in our Federal Government and focus on replacing the ones at most critical risk.

Senator UDALL. Mr. Barlow, please?

Mr. BARLOW. I think the biggest challenge is really understanding the vulnerability of any system. There are plenty of brand new systems that come out that are chock full of vulnerabilities. Now, obviously, the older things get, the more likely they are to degrade. One of the things, though, I think we've been talking about as a group today is the importance of making sure that systems can, for their useful lifetime, be updated.

Now, whether that useful lifetime has exceeded itself in the commercial sector or not is really immaterial. It's about making sure that we have the security posture; the vulnerability assessments in place; we understand the risk; we're using a security framework so we've got breadth and depth in our security posture; and, last and probably the most important thing that people often forget about, that you've got a relationship with incident response forces, whether that's in the government or private sector, that can monitor that environment continuously and respond when there is a problem.

Senator UDALL. Thank you very much.

Thanks, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Udall.

Senator Fischer?

**STATEMENT OF HON. DEB FISCHER,
U.S. SENATOR FROM NEBRASKA**

Senator FISCHER. Thank you, Mr. Chairman.

Mr. Grobman, in your written testimony, you state that manufacturers of connected devices need to think about security by design—we've heard some comments here today—so that these protocols will be in the devices from the beginning rather than adding them later on. How can companies that are innovating in the Internet of Things space mitigate the burdens of security by design? For example, when is the use of patches or other security upgrades sufficient to combat those new threats that we face really every single day, as opposed to redesigning the devices wholesale in the future?

Mr. GROBMAN. So, very much like the NIST framework coming up with a specific list of areas that an organization must pay attention to, that is the same sort of process that we need to instill in our embedded Internet of Things devices. There's a set of requirements that almost any IoT device will have, even though those requirements and what makes up those requirements will evolve over time, so, just as an example, the general category of field repair ability, making sure that when a device is installed in the field that it is possible to get the updates to it in a secure manner.

One of the large problems that we do recognize, though, is what is reasonable for a manufacturer to take care of a device. If a manufacturer sells a device for \$30 with a 3-year warranty, if a vulnerability is discovered in year seven, are they still subject to being required to deploy fixes? What about in the case where manufacturers no longer exist, and we are still left with millions of vulnerable devices? Very challenging problems.

Senator FISCHER. Do you have suggestions on how we're supposed to handle that, especially in the future, when companies come and go, when we see technology being developed so quickly and the innovation taking place? How are we going to address that? Because those devices will still be out there.

Mr. GROBMAN. I think one of the most important things that we can do in the near term is have consumers think about security in much of the same way that they think about reliability or safety in other products. We really need to raise awareness that security in all devices is key. I do think there are some real practical challenges, though, especially given the global nature of product devel-

opment, that products developed in other countries will not have the same forethought.

Senator FISCHER. That leads me to my next question, Mr. Ganesan. I expect that many companies that you work with are investing in the Internet of Things and you're developing all these great innovative products in the area, and we're looking to make sure that these devices are secure and they're not going to be vulnerable to cyber threats.

We've heard about the importance of the security of the supply chain. We've heard about making sure that the systems can be updated during their useful lifetimes. That said, I'm concerned that innovation is going to be hindered because consumers aren't going to buy these devices because they're going to be very concerned about security.

So how do you believe the investment into the Internet of Things has been deterred because of those security concerns, and what can the private sector do to make sure that we ensure that the investment that we're seeing in the Internet of Things is going to continue?

Mr. GANESAN. Excellent question, Senator Fischer, and I agree with you that making sure that we have a secure infrastructure, a secure framework for IoT is going to be critical for adoption. One of the market-based approaches we have taken at Menlo is we have funded a company called BitSight that does security ratings, and one of the things that BitSight does is actually like Moody's and Standard & Poor's. It gives you a security score at a company level and at individual product levels so that people can get a sense.

I like market-based approaches like that where people can have a feedback loop, where you can get a score, you can improve it, and consumers have visibility to that so that they can decide whether they want to work with a certain company or not, if they want to work with certain products or not.

Senator FISCHER. So as long as we can see the private sector stepping up and providing those security options for consumers, you believe that that development in the Internet of Things and the reliability that consumers would feel in that development would be sufficient?

Mr. GANESAN. I do, Senator.

Senator FISCHER. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Fischer.

Senator Hassan?

STATEMENT OF HON. MAGGIE HASSAN, U.S. SENATOR FROM NEW HAMPSHIRE

Senator HASSAN. Thank you, Mr. Chairman, and good day to all of our panelists. I thank you so much for being here.

I want to follow on a little bit of what Senator Fischer was beginning to discuss. Last December, a company in my state, Dyn, in Manchester experienced a series of distributed denial of service attacks. Since Dyn directs global Internet traffic for some of the top social media, e-mail, and streaming services, the impact of the attack, as I'm sure all of you know, was felt throughout the country. Perhaps most unsettling about this attack was that hackers turned

everyday Internet devices into a force multiplier that targeted Dyn, a very sophisticated technology company. So this isn't just about consumers being disrupted.

So, Mr. Rosenbach, if groups of criminal hackers can mobilize the Internet of Things to help advance an attack like this, then, clearly, countries like Russia and their teams of state-backed hackers could use the Internet of Things to mobilize a far more catastrophic attack. So what are your thoughts about what we can do to prevent against state-sponsored attacks of this nature?

Mr. ROSENBACH. Yes, ma'am. So this is a great example of where the Internet of Things has a dark side that the government needs to play some role in, because you can't expect a firm like that—if it were the Russians or the Chinese or the Iranians, who are also very active in putting together the bot networks—to be defending itself. So it doesn't mean that it should always be the Department of Defense. In fact, we should probably be the last people you call in, because we want to be very respectful of civil liberties and the constitutional tradition.

But there needs to be a hard conversation about when the government is going to defend a firm like that in New Hampshire, because, otherwise, the investment they would need to make in defending themselves will put them out of business. That's not the role that they should be in. There is a role for government when it comes to state-based attacks.

Senator HASSAN. Thanks.

Mr. Barlow?

Mr. BARLOW. Well, Senator, I think one of the other challenges we have to recognize that was very unique about the Dyn attack is that many of the devices that were used were everything from everyday nanny cameras, however, they had the default user IDs and passwords on these devices. Now, it's incredibly easy to write a script to go scan the internet looking for these devices and then check if it is—you know, literally, if the password is still admin and password.

You know, one of the challenges is the bad guys can use these tools to not only scan, but to go try to log in to these devices and then identify them for potential inclusion in their botnet. The good guys can't do that, because the minute I try to log in with a default user ID and password, I'm breaking the law.

Now, I'm not saying I want to go enter into these devices, but I certainly—whether it's working with government or working with other private sector entities, I want to know where these devices are, so we can potentially notify the manufacturers, who probably have some responsibility here, notify the end users or where these are deployed, or worse yet, just identify these devices so they can be black listed so they can't be used in an attack like this. That's a critical area where the threat has evolved past the good intentions of the prior law.

Senator HASSAN. Well, thank you. I want to just take my last minute or so to talk a little bit more about bots. I am referencing a McClatchy report on this from earlier this week that the FBI is investigating Russia's use of bots to blitz social media and try to influence the public discourse surrounding the 2016 Presidential election. So if the allegations are true, it shows that Russia had

made use of a powerful tool to disseminate misinformation and fabricated stories on truly a mass scale.

The University of Oxford study found that on Twitter during the period of October 9 through 12, 2016, there were over 850,000 tweets from suspected bot accounts. It would seem that some of the emerging technology discussed today could be used to counter the proliferation of Twitter bots and the Russian misinformation campaign.

So, again, I'll start with you, Mr. Rosenbach. Can you please take a minute and discuss how we can use these technologies to address this problem?

Mr. ROSENBAACH. We have experience in this in the government from a bot-based campaign that the Iranians conducted against U.S. banks several years ago. So the technical solution to taking out bot networks is not actually that difficult. But, one, you need the willingness to do it, you need to make sure that it's transparent under the law, and then you have to work with a lot of international partners because the bot network on its face is located in many different countries around the world.

But that is where there's a role for the government to play, because, otherwise, it won't happen, and you can't expect one private sector firm to counter the Russian government's effort to influence our elections.

Senator HASSAN. Thank you. Anyone else want to comment?

[No verbal response.]

Senator HASSAN. Well, then, thank you very much.

And thank you, Mr. Chair.

The CHAIRMAN. Thank you, Senator Hassan.

Senator Blumenthal?

**STATEMENT OF HON. RICHARD BLUMENTHAL,
U.S. SENATOR FROM CONNECTICUT**

Senator BLUMENTHAL. Thank you, Mr. Chairman.

We've talked a little bit, I think, about the kinds of dangers posed by devices that are insufficiently secure in the Internet of Things world, and as we usher in this new era, there will be an explosion of devices that are connected to the internet. Everything will be. Cisco has said 50 billion things will be connected to the Internet by 2020. We're not talking about something in the far distant future. It's upon us now.

But we're only as strong as the weakest link. We know that from experience. And even if only a tiny percentage of these devices have weak cybersecurity, they can cause very significant harm to consumer privacy and security and even to national security.

In October, an array of popular websites and services, including Amazon, PayPal, *The New York Times*, and Twitter, were shut down, and it turned out that the shutdown was the result of a hack. The hack was powered by multiple massive botnets which operate by commandeering thousands, tens of thousands, of vulnerable devices, baby monitors, routers, printers, DVRs, the most common household devices, seemingly often the most innocent, and the devices were directed to conduct criminal activity unbeknownst to the consumer. I'm telling you something everybody on this panel knows. Very few Americans know.

The question I have is: Shouldn't insecure devices be regarded as, in effect, defective products, consumer products that are perhaps as dangerous as a toy with small parts that children may swallow, or blinds that can strangle them because they're improperly constructed, or baby toys that have lead? In other words, shouldn't they be subject to recall, taken off shelves, if they're insufficiently secure, and out of consumers' homes if they can't be patched through to a software or firmware update?

So let me ask the panel, in no particular order. But I notice that you have your hand up, so go ahead.

Mr. GROBMAN. So I think there are some differences that we need to be very aware of in looking at IoT devices as compared to traditional consumer devices. One is their global nature. In the example that you gave with a toy having lead, it is only going to do damage within its direct vicinity, whereas the challenge that we have, such as in the Mirai attack, it wasn't just machines that were located in the U.S. or IoT devices that were located in the U.S. executing the attack, but from all over the world.

My team actually ran a test 2 months ago where we created a fictitious vulnerable device that we put on an open network in January. Within a minute and 6 seconds, it was infected with the same botnet that ultimately took down the sites that you mentioned. We ran the test from Amsterdam, and we were attacked from Vietnam, not the country, but from some infected DVR that happened to be in Vietnam.

So although, I think, on the surface, thinking about some of the correlations to the physical world are good things to think about, I do think there are many, many differences that we need to pay attention to.

Senator BLUMENTHAL. Why don't we begin at that side and just go down the panel.

Mr. BARLOW. Thank you, Senator. So I think at the most basic level, if it connects to the internet, you've got to have a way to secure it and update it for the lifetime of the device, hard stop. Now, what that may evolve into is some sort of freshness date or some sort of subscription date for the device.

The challenge I think we face is that no matter how much effort and work you put into securing the device when it's originally produced—let's take a thermostat installed in someone's home. Who knows what vulnerabilities, what techniques, what solutions are going to be available 10, 20 years down the road? So, you know, that's part of what we've really got to think about, is the time factor of how long is that device viable and how is it going to be updated.

Mr. GANESAN. Very briefly, I think the challenge from a regulatory framework is even if you could have some sort of guidelines for the U.S., there are webcams in Singapore that could still affect companies here, and there would be no way to figure out how to manage that. So we don't want to do something that will unfairly put burdens on American companies that doesn't apply globally.

Mr. HARKINS. Just to add, I agree with all of what was said here, and I think it's also important to note that beyond just updating, there is the potential for patching. But, again, as Mr. Grobman indicated, patching after the fact, long after the fact, might be dif-

ficult. So the real question becomes not only updating, but really how do we protect it. Updating is one potential mechanism to protection, not the only mechanism.

Mr. ROSENBACH. Sir, this isn't my area of expertise, but I'd say if you could find a way to put more on individuals and make individuals responsible for some of their own cybersecurity, that would be another way to turn it around, that probably even under the complexities of litigation law would get at what you're going to.

Senator BLUMENTHAL. I very much appreciate these answers. I recognize that my question is a very complex and broad one, and in a couple of minutes you've suggested some areas, some directions, we should go. But I agree that it is a global problem. We don't want to put American companies at any disadvantage.

I also agree that individuals bear a part of the responsibility, and I agree that, fundamentally, the problem may be viewed as different from a toy that just affects a single child or family. Maybe that makes it even more dangerous, although one life at risk could be judged to be as important—certainly as important as a global shutdown of Internet devices.

But I think we're just beginning to grapple with this issue, and I'm suggesting a recall type of procedure, because very soon, it will be not just a matter of individual security or family security or town or city, but it will be truly national security, and, indeed, it already is, as we've seen from some of the attacks mentioned here—Russians—you mentioned Vietnam, a hacker in Vietnam. We're at the point where we don't know whether that hacker is a free agent or somebody operating under the auspices of a government, not to say about Vietnam, but certainly about Russia. That's been the experience.

So we're very much in dangerous uncharted waters, and I hope we'll continue this conversation.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Blumenthal.

Let me just ask—as I understand it, blockchain relies on a decentralized or distributed database of transactions. And, Mr. Barlow, you testified that blockchain has potential applications for the sharing of cyber threat intelligence because it maintains data security and integrity without revealing its source. How could this technology facilitate information sharing between industry and Federal agencies and within industry-specific information sharing and analysis centers?

Mr. BARLOW. Thank you, Mr. Chairman. That's an excellent question. I think one of the things we have to recognize is whether we're talking about, let's say, a large bank or an energy company or even a government, everyone has concerns about people looking at the threat information they're sharing and trying to decipher other activities, you know. What's the acquisition they're about to maybe—the company they're about to acquire or a particular form of intelligence they may be under.

One of the things that we look at blockchain with a lot of optimism around is the ability to aggregate that data together. And when you aggregate it together, all of a sudden, even the anonymous becomes even more anonymous. But any time you have a big collection of data, you really need to be able to maintain that rep-

utation. You don't want people just throwing things in there that are either duplicates or throwing out extraneous information or, worse yet, false flags.

One of the real promises of blockchain is it gives people the ability to share with cryptographic integrity and integrity around the reputation of the source, but with only a few people, if any, actually knowing who the source is. So that's one of the things we really look at, because you could take government data, you could take data from a large bank, and you could take data even from small boutique cybersecurity firms, aggregate it all together, and it would be nearly impossible to figure out who presented this data into the collective, but you'd understand that it's a high reputation source and that you need to take action immediately.

The CHAIRMAN. Mr. Grobman, Intel is currently conducting research on the future deployment of blockchain for security applications. What are some of the current hardware limitations that you have encountered?

Mr. GROBMAN. So one of the things that we're looking to do is combine what blockchain can do from an infrastructure perspective, so providing greater levels of resiliency and immutability on the infrastructure side along with greater levels of trust on the device that actually creates the data to begin with. So there are a number of hardware technologies that are in Intel's upcoming hardware lines that make it so you can cryptographically sign data, secure data before it moves into the blockchain. So it's really the combination of those two.

One note just on Mr. Barlow's answer on threat intelligence. I do think this is a very good example of using hardware to be able to ensure how the data was collected, has a high degree of integrity, along with blockchain, but also recognize some of the challenges inherent in threat intelligence-sharing. It's one of the things that we call a free-rider problem, meaning that everybody wants threat intelligence, but there's generally very little incentive to give up threat intelligence.

So figuring out how to not only remove the barriers, but actually create incentives to provide threat intelligence, much like your point on cyber insurance, is a good way for us to think about the problem at the next level.

The CHAIRMAN. Mr. Ganesan, we often hear the terms, AI and automation, mistakenly used interchangeably. Currently, to what extent are the cybersecurity startups and companies that you encounter actually using AI and machine learning, and how much further do they have to go?

Mr. GANESAN. Senator, I think there has been a lot of progress in AI, in the sense that I would say that even a few years ago, a lot of the things that we do today were not possible, and that's a combination of things including having great cloud services, having data, and then having sophisticated algorithms. So where I think the progress is being made is in very vertical AI use cases.

Specifically, I think the exciting areas to me are on automation of security alerts. There are just too many security alerts in the world. There are not enough people in the world to run down every one of these alerts. Every one of these great companies create

alerts that go out, and I think what AI has been good at focusing on is vertical problems where they can go in and automate.

So I think of the progress being made as man plus machine as opposed to man versus machine, and so here AI is going to work on the mundane stuff so that our security professionals can focus on the higher value threat.

The CHAIRMAN. Yes, sir?

Mr. BARLOW. The average security operations center sees 200,000 security events a day. A large bank would be several millions. Human beings simply can't get through that. So one of the real promises of artificial intelligence above and beyond cognitive systems is the ability to help security operations professionals dig through that.

In our early findings with our Watson project, we're finding that Watson's capabilities are 60 times faster than manual complex analysis, with 10 times more actionable indicators identified. It's bringing that kind of ability to sift through this data that can really take the threat intelligence that we all need to share and help make an actionable difference.

The CHAIRMAN. I think we could all use a Watson in our office, probably, to keep sorting all these things out that we have coming at us all the time.

Let me just ask a generic question, and that has to do with if you thought about, kind of, what is the thing that keeps you up at night, biggest fear, biggest concern, and then maybe to put a brighter note on it, kind of, what your biggest hope and opportunity is as well. But just kind of a general question, but as you think about the space that you work in, what is it that concerns you the most? What's the biggest fear?

Mr. BARLOW. My biggest fear is that as security professionals, we often become very enamored with the problem. It's very easy and very quick to focus on things like nation-state activity, espionage, and all these types of things, which, let's face it, at the end of the day are accepted international practices. What I worry about is we also have to recognize the level of organized crime in this neighborhood is unbelievable, and I really firmly believe that if we work together, which is something that we can all agree on regardless of which side of the political aisle anyone sits on, that the organized crime has got to go, then we can make a real and substantial difference. And then the only thing left to focus on is the nation-state activity.

Now, the positive side of this, as much as we talk about all the negative, is this is fueling an enormous new economy of new talent, of STEM skills, of high-paying jobs, and I think it's incumbent on all of us to work together to ensure more of that work, more of that skill, more of that new talent lands here in the United States.

The CHAIRMAN. Mr. Ganesan?

Mr. GANESAN. Senator, my biggest fear is critical infrastructure. There are many problems we can solve individually, but critical infrastructure is something that can only be protected at the government level, and, therefore, that would be my biggest fear.

But my biggest hope and optimism is the fact that we have the best entrepreneurial ecosystem in the world by far. Every major security innovation, every major cybersecurity company are funded

and created in America. We have the world's best venture capital system and the best set of entrepreneurs. What we just need to do is to make sure that we enable these people, make sure we can attract the best and brightest to come to this country, that we have the capital available for them to fund it, and give them the room to grow and innovate, because when we do that, we can solve anything.

Mr. GROBMAN. I think my biggest concern is that what we call the threat surface area continues to grow. So much of what our discussion was on today dealt with new areas of innovation, whether it was self-driving cars or automation in factories or connecting our critical infrastructure capabilities. The implications of a cyber attack on any of those would be catastrophic. But yet our traditional systems are not taking care of themselves. So it's not that we can shift our focus from the old to the new, but rather we're forced to expand our comprehension of what we need to secure in order to survive as a nation.

What gives me hope is this concept that has been discussed a bit today on human-machine teaming, where we use technology to amplify the effectiveness of our cyber warriors, our cyber defenders, that will ultimately enable us to secure this new scale of capabilities that we ultimately need to defend.

The CHAIRMAN. Mr. Harkins?

Mr. HARKINS. My biggest fear, honestly, is that we perpetuate the cyber risk curve that we see today, and that we don't fundamentally address the problem, and we continue to be reactive and responsive at a cost to our business, at a cost to our customers, at a cost to society.

My biggest hope, though, honestly, even in this discussion today—I've long believed that the biggest vulnerability we face today and in the future is the misperception of risk. I think we've misperceived it 10, 15 years ago, and I think by having the dialogs like we're having today, we'll start a better discussion. We'll better understand where new technologies, the blockchain, quantum computing, artificial intelligence, and machine learning, not only can add benefit in other areas of the digital economy, but can be used and tuned to prevent issues from occurring to begin with and then better detect and respond to them if damage was to occur.

Mr. ROSENBACH. Yes, sir. I would say what keeps me awake is that right now, we're watching the evolution of cyber warfare, something where there are hacks and the spread of disinformation, and that if something bad were to happen either to the democratic system or to our financial system in which trust in those two systems is undermined to the point that the U.S. loses two things that are incredibly valued, and that then the country's reaction to those things and maybe even the Congress', if I could be so candid, would be so strong that it might actually stifle some of the innovation and everything good that is happening right now. So that keeps me awake.

The thing that always makes me feel good—in particular, when I was in the Pentagon, if you go to CYBERCOM and you go to NSA, and you see really talented, hardworking soldiers and civilians who are very talented and could go make several hundred thousand dollars on the outside, but they want to stay there, they

want to keep working on it, they want to defend duty networks, and they want to go after the bad guys, that always gives me hope. The CHAIRMAN. Good. All right. Good answers. Senator Cruz?

**STATEMENT OF HON. TED CRUZ,
U.S. SENATOR FROM TEXAS**

Senator CRUZ. Thank you, Mr. Chairman. I'd like to thank each of the witnesses for being here today, and, Mr. Chairman, thank you for holding this important hearing.

Last November, my Subcommittee on Space, Science, and Competitiveness held the first congressional hearings on artificial intelligence, both the opportunities and the challenges and threats posed by artificial intelligence. Among the promise artificial intelligence presents is the opportunity to unleash a technological revolution that the world has not seen since the creation of the internet, and it could impact every sector of our economy.

A 2016 Accenture report predicted that artificial intelligence could double annual economic growth rates by 2035 and boost labor productivity up to 40 percent. So these are exciting new opportunities for our economy, but at the same time, this technology produces challenges that could have very significant impacts in labor markets and a real need to secure the privacy of individuals and to guard against threats, in particular, in the cybersecurity space.

In an interview with *Wired* magazine last year, President Obama stated, "Then there could be an algorithm that said, 'Go penetrate the nuclear codes and figure out how to launch some missiles.' If that's its only job, if it's self-teaching, and it's just a really effective algorithm, then you've got problems. I think my directive to my national security team is don't worry as much about machines taking over the world. Worry about the capacity of either non-state actors or hostile actors to penetrate systems, and in that sense, it is not conceptually different than a lot of the cybersecurity work we're doing."

My question for each of you is: What impact is artificial intelligence having on how we currently approach cybersecurity, and how will that approach have to change over the next decade?

Mr. GROBMAN. So, Senator, I think one of the points you make is a very good one, which is, we can't be naïve to think that artificial intelligence will only be used by defenders, and one of the things that we see in cybersecurity is very often the attackers are able to implement new technologies more rapidly. So having an attacker use artificial intelligence for what we call victim selection, essentially the scenario you outlined, where it's identifying the place in an organization or an environment where they'll be most successful, is some of what we're starting to see today.

The good news is if we recognize that and start planning for the bad actors to have that weaponry in their arsenal today, we can build strong defenses and most effectively use the same technology to build strong capabilities as well, and that's what a lot of us at the table are doing in our businesses to try to get ready for those scenarios.

Mr. HARKINS. Senator Cruz, I think it's important in what you talked about in terms of the potential, and I agree with Mr.

Grobman. But I also think that we've proven today that we can use artificial intelligence to stop malicious code from happening. I think it's also possible to use artificial intelligence and machine learning to deal with the identity problem and do continuous authentication to know that Malcolm is Malcolm, his machine is his machine, and allow him to do the things that he needs to do as a user.

I also think it's possible to use artificial intelligence and machine learning to disrupt and stop denial of service attacks, like what we saw with Dyn. I think we have to use these technologies, use the advanced algorithms, use the math and the science, and place them in the right spots to really get at the heart of the problems and better predict and prevent these problems to begin with. And then if we can't, because you cannot eliminate the full vulnerabilities, then you have to use that technology to speed up the detection and response and mitigate and slow the potential for harm.

Senator CRUZ. One of the threats that we heard testimony about at the November hearing on artificial intelligence was a cybersecurity threat as more and more decisionmaking is based on big data, a cybersecurity threat that doesn't come in and shut down a system in a way that it's obvious that it has been hacked, but rather that goes and alters the dataset that is being relied upon for artificial intelligence to make decisionmaking and to alter the dataset in a way that it's not immediately evident, but changes the decision-making in a way that could have significant consequences. That struck me as a particularly difficult form of cyber threat to respond to. I'd be interested in your comments.

Mr. GROBMAN. So I think one of the things that we see in any new cyber defense technology, is as soon as it gains traction in the industry, the attackers look for ways to create countermeasures, evasion tactics. A few years ago, the industry was very focused on what we call sandbox detonation, essentially trying to run an unknown executable in a safe environment to see if it had malicious behavior. Very quickly, the adversaries would try to fingerprint to detect "am I running in that environment." And I think we can expect that same mindset for the adversaries as the industry embraces AI-based defenses.

So one of the things we're looking at is really understanding the attacker's point of view. How will they use machine learning poisoning? How will they poison the models? How will they force defenders to recalibrate their defenses because they sent a lot of false positives that are very costly for their operations center? And really recognizing that at the beginning will allow us to build more resilient capabilities.

Mr. GANESAN. Senator Cruz, if I can add a different dimension, we are, I think, in the golden age of AI. In the next probably 15 to 20 years, we'll get to the point where we can do a lot of really impressive things. But now it's a war for talent. We need to make sure that we get the best AI folks. From where I come from in Silicon Valley, Facebook, Google—they spend—I'm not kidding you—millions of dollars trying to get the best AI folks to join them.

This global talent is spread all over. My point of view is let's figure out a way to make sure that we can get the best AI talent from all over the world to come here to our universities and, more importantly, stay here and create companies here.

Mr. HARKINS. Senator Cruz, specific to your question around a data integrity attack, we have to look at how would a data integrity attack occur. One would be I own your system, and I own the data base, which means malicious code was placed on that. So the way to mitigate that is to prevent malicious code from executing.

The other way that would be simply there is I own your identity, or I'm an insider and I changed the data. And, again, there are ways to do the authentication to validate the individual, and then there's backend detection on the data integrity, and I think—as was mentioned earlier with blockchaining, I think that's a great way to ensure some level of data integrity out in the future and use that for critical data to give you a higher level of trust.

Mr. BARLOW. I think one of the challenges in the question you posed is that there's a lot of data behind that, and you're not looking for the needle in the haystack. There's no one sending up a big red flare. You're trying to find a needle in a stack of needles with everything else that's going on. And, interestingly enough, I think the solution to the problem is also artificial intelligence and cognitive systems.

I've had the opportunity over the last year to watch Watson grow up, and, literally, it was like watching a child grow up. There was an early day where we—it couldn't understand what ransomware was, because it wasn't in the dictionary. So it thought ransomware was a city. Right? OK. Well, I can kind of see how it would make that mistake. And then we got to the point, almost like it was in college. We were grading papers, going, "Hey, you got an A on this one. This one, you still need a little work to do."

But we're at the point now where we're putting this up against talented security teams, augmenting their skills, and what it's doing is giving them that peripheral awareness to go, "Hey, something very unusual and obscure"—very much to your example, Senator—"happened over here. Why is that happening? Have I seen it before? Is there a research paper that talks about this? Is there another threat intelligence company that's identifying this?" And it's bringing that level of awareness right to the surface, but with an evidence-based conclusion, and that, ultimately, is the type of thing we need to combat, the exact same threat.

Senator CRUZ. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Cruz.

I think we've exhausted members and their questions, so thank you all very much, panel.

I want to, before we wrap up, ask unanimous consent to place in the record three pieces of additional testimony. The first is from Professors Scott Shackelford and Steve Myers of Indiana University. The second is from Larry Clinton, the President and CEO of the Internet Security Alliance. The third is from Theresa Payton, the CEO of Fortalice Solutions. So without objection, it'll be so ordered.

[The information referred to follows:]

PREPARED STATEMENT OF PROFESSORS SCOTT SHACKELFORD AND STEVE MYERS,
INDIANA UNIVERSITY

Chairman Thune, Ranking Member Nelson, distinguished members of the Committee, thank you for the opportunity to offer this statement for the record to help

inform your Committee's important work with regard to the risks and opportunities of emerging fields for cybersecurity.

We are professors at Indiana University-Bloomington engaged in cybersecurity and emerging technologies research. Our work touches on a number of fields of interest to this hearing, including Internet of Things (IoT) security, cryptography, the promise and pitfalls of blockchain technology, and supply chain cybersecurity. For purposes of this statement, we will limit our remarks to the IoT context.

Introducing the Internet of Broken Things

On July 21, 2015, there was a car crash. This in and of itself is not newsworthy given that there are, unfortunately, some 15,000 car accidents daily in the United States.¹ What made this episode different, though, was the fact that this crash was not the result of drunk driving or human error; rather, code was to blame.² Hackers Charlie Miller and Chris Valasek took advantage of fundamental flaws, so-called "zero-day exploits,"³ in the software running a Jeep Cherokee and used these entry points to turn on the car's air conditioning, change the radio station while cranking the volume, turn on the windshield wipers, display a picture of themselves on the car's navigation screen, and eventually disable the car's transmission.⁴ All of this was done from a laptop some ten miles away from the targeted Cherokee.⁵ And this episode was far from unique. Flash forward to late 2016 and the appearance of the Mirai botnet, which paralyzed much of the web in late 2016 by overwhelming Dyn, an Internet-services firm, in an attack that has shown an even harsher spotlight on IoT insecurities.

Together these and other instances highlight the extent to which smart products hold the promise to revolutionize business and society. In sum, from 2013 to 2020, Microsoft has estimated that the number of Internet-enabled devices is expected to increase from 11 to 50 billion, though estimates vary with Morgan Stanley predicting 75 billion such devices in existence by 2020.⁶ To substantiate the coming wave, Samsung recently announced that *all* of its products would be connected to

Professor Scott Shackelford

Associate Professor, Indiana University Kelley School of Business
Cybersecurity Risk Management Program Chair, Indiana University-Bloomington
Director, Ostrom Workshop Program on Cybersecurity and Internet Governance
Affiliate, Harvard Kennedy School Belfer Center Cyber Security Project
Affiliated Scholar, Stanford Center for Internet and Society

Professor Steve Myers

Associate Professor of Computer Science & Security Programs Director
Indiana University School of Informatics and Computing

*This statement was adapted from Scott J. Shackelford et al., *When Toasters Attack: Enhancing the 'Security of Things' through Polycentric Governance*, 2017 UNIV. OF ILL. L. REV. 415 (2017); Scott J. Shackelford, *When Toasters Attack: 5 Steps to Improve the Security of Things*, CYBER MAGAZINE (Sept. 8, 2016), <http://magazine.milcyber.org/stories/whentoastersattack5stepstoimprovethesecurityofthings>; Scott J. Shackelford, *Opinion: How to Fix an Internet of Broken Things*, CHRISTIAN SCIENCE MONITOR PASSCODE (Oct. 26, 2016), <http://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/1026/Opinion-How-to-fix-an-internet-of-broken-things>; L.Jean Camp et al., *TWC: Large: Collaborative: Living in the Internet of Things*, *Proposal for NSF Award #1565375*.

¹See Nat'l Highway Traffic Safety Admin., *Fatality Analysis Reporting System*, <http://www-fars.nhtsa.dot.gov/Main/index.aspx> (last visited Aug. 6, 2015).

²See Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me In It*, WIRED (July 21, 2015), <http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.

³In a zero-day attack, a hacker creates an exploit before the vendor knows about the vulnerability, so the attack base is broader. There is little that users can do to slow down zero-days once they are unleashed, so an attacker "can wreak maximum havoc." Gregg Keizer, *Microsoft's Reaction to Flame Shows Seriousness of 'Holy Grail' Hack*, COMPUTERWORLD (June 7, 2012), http://www.computerworld.com/s/article/9227860/Microsoft_s_reaction_to_Flame_shows_seriousness_of_Holy_Grail_hack.

⁴See Andy Greenberg, *Twitter Hires Elite Apple Hacker Charlie Miller To Beef Up Its Security Team*, FORBES (Sept. 14, 2012), <http://www.forbes.com/sites/andygreenberg/2012/09/14/twitter-snags-elite-apple-hacker-charlie-miller-to-beef-up-its-security-team/>. Christopher Valasek is "the Director of Security Intelligence at IOActive, an industry leader in comprehensive computer security services." Chris Valasek, RSA Conf., <http://www.rsaconference.com/speakers/chris-valasek> (last visited Aug. 6, 2015).

⁵See Greenberg, *supra* note 2.

⁶See Tony Donava, *Morgan Stanley: 75 Billion Devices Will Be Connected to The Internet of Things By 2020*, BUS. INSIDER (Oct. 2, 2013), <http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10#ixzz3i4CApJsg>.

the Internet by 2020.⁷ Regardless of the number, the end result looks to be a mind-boggling explosion in Internet connected stuff. But the burning question now is whether security can scale alongside the fast pace of innovation.

Enhancing the Security of Things

What role do policymakers have to help enhance IoT security? We have outlined eight areas for your consideration, including a number of IoT specific initiatives:

1. First, we need more cooperation amongst stakeholders, including information sharing within defined boundaries to build trust, along with graduated sanctions being in place for rule breakers. The auto industry Information Sharing and Analysis Center (ISAC) is one example of this approach that should be replicated in other IoT sectors, though broader IoT Information Sharing and Analysis Organizations (ISAOs) would also be beneficial to break down artificial silos and spread cyber threat data and best practices more widely.
2. Second, Congress should consider certain baseline standards for IoT devices, such as the ability to securely and easily accept security updates, and only from authenticated and trusted channels. An initial model is the National Institute for Standards and Technology's (NIST) Cybersecurity Framework, along with its work on Cyber-Physical Systems. Over time, these standards could help establish a standard of IoT cybersecurity care, including new approaches to proactive cybersecurity measures.
3. Third, there is ongoing benefit in flexible, guidance-driven frameworks in the IoT context over prescriptive regulation given the fast-evolving nature of these technologies. Still, a range of policy options are available to incentivize cybersecurity investments, ranging from R&D tax breaks to public bug bounty programs and grants to help establish cybersecurity clinic collaborations between firms, research universities, and community colleges across the Nation. Further incentives include liability limitation for certain types of information sharing in the IoT context,⁸ technical assistance for critical IoT sectors, and offering priority consideration to certain Federal grants all serve as examples of such incentives.⁹ We note that security is not currently a property of products that is easily signaled to or understood by consumers, and so it is difficult, at least initially, for consumers to make informed decisions on security, and thus for the market to naturally select towards more secure products. We also recommend that more attention should be paid to the intersection of IoT and the need to secure supply chains. Since IT systems control everything from phones to factories, ensuring these systems are secure is of vital importance to the global economy. Yet this is a daunting proposition given varying sources of insecurity, from malicious—a 2012 Microsoft report found malware being installed in PCs at factories in China—to conflicting commercial incentives, such as Lenovo's installation of advertising software that weaken security in 2015. Regardless, manufacturers will have no ability to assert basic security properties of their products if supply chains are not considered.
4. Fourth, IoT providers should be encouraged to undertake good governance best practices, which can be accomplished by effective monitoring of IoT peers and an active role for civil society in shaming outliers. The power of supply chains and private contractual relationships could be brought to bear to help encourage the dissemination of best practices, such as firms requiring NIST Cybersecurity Framework compliance from their suppliers. Similarly, an active dialogue between public and private sector supply chain governance is needed.
5. Fifth, government should be willing to allow industry to react to data breaches without overly broad, harsh or punitive fines, except in egregious circumstances as has begun to be defined in the U.S. context through FTC Act Section 5(a) litigation. Firms should also be encouraged to make use of existing

⁷See Rachel Metz, *CES 2015: The Internet of Just About Everything*, TECH. REV. (Jan. 6, 2015), <http://www.technologyreview.com/news/533941/ces-2015-the-internet-of-just-about-everything/>.

⁸This is already happening to an extent with the U.S. Government encouraging automobile manufacturers to work with one another through a new Information Sharing and Analysis Center and with consumers and the government to identify and share cybersecurity best practices. See Pete Bigelow, *18 Automakers Agree on New Safety Pact with Regulators*, AUTO BLOG (Jan. 15, 2015), <http://www.autoblog.com/2016/01/15/18-automakers-agree-new-safety-pact/>.

⁹See Michael Daniel, *Incentives to Support Adoption of the Cybersecurity Framework*, WHITE HOUSE (Aug. 6, 2013), <https://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework>.

tools from other contexts, such as integrated reporting schemes, to better inform cybersecurity decision-making.

6. Sixth, government should consider the effects that emergent properties of IoT attacks can have on populations when large numbers of IoT devices are simultaneously attacked. For instance, we note a few Internet devices being infected with a botnet provides little security threat, but a large deployment of such devices provides attackers the ability to disrupt the services of even the largest Internet content providers. Similarly, the ability of attackers to disrupt and break a single IoT heating system in a home may be a nuisance, but the ability of attackers to disrupt a large fraction of a community's heating systems in the midst of winter could be considered a local emergency. This is true, if local inventory is not sufficient to replace broken components, or if the time necessary to perform repairs is significant, and the local workforce is insufficient to supply surging demand. We note that emergent attacks on a wide variety of potential IoT products lead to outcomes that can be worrisome. Some simple examples include: (i) if many cars can be stopped in a localized area, then roads can become impassible; (ii) if smart meters can be bricked, then the full communities may lose power; and, (iii) if refrigeration can be affected, communities may lose perishable food stuffs.¹⁰ Emergent properties of such attacks may necessitate the rethinking of what constitutes critical infrastructure, or the need for minimum security and safety standards in some IoT categories.
7. Seventh, government should consider the effects of IoT policy not just on device manufacturers and consumers, but on integrators and managers. IoT deployment ecosystems may comprise more than just IoT devices and various stakeholders IoT devices' environments; indeed, there may exist third parties that assist with the integration and management of IoT devices within a larger IoT ecosystem. These integrators already play a significant role in corporate IoT deployments (for example, building control systems for facilities), and we envision integrators will soon play a critical role in many domestic IoT deployments as well. As an early precursor to such domestic IoT integrators, the Xfinity ISP currently offers its Home package—a suite of home security and automation technologies. However, it is clear that many of the large corporate technology corporations would like to sell services that incorporate consumer IoT devices—both monitoring and supporting them. Ensuring that government policy allows and ensures such integrators to securely and privately support products while interacting with many vendors will ensure more consumer choice and allow for more competitive markets, and prevent vendor lock-in. We support this, even though it will admittedly make security technically more difficult to achieve.
8. Eighth, government policy on IoT security needs to consider IoT devices in their complete lifecycles. This lifecycle begins with product conception and development; next is device acquisition; the lifecycle proceeds to device deployment; and, after deployment, the lifecycle proceeds to device administration and maintenance. In some cases, the owner of an IoT device might transfer the device to another party, in which case the lifecycle loops back to device acquisition. Eventually, the device manufacturer will end the supported life of the device, thereby rendering that device a “zombie”—where new attacks may be found in widely deployed devices, but manufacturers are no longer willing to support the product for economic reasons, leaving large deployed bases of knowingly insecure products. Security concerns can arise anywhere in this lifecycle, and hence a holistic approach to IoT security must consider the full lifecycle. Additionally, the product lifecycles for many IoT durable goods (e.g., kitchen appliances, thermostats, etc. . . .) is much longer than the typical high-tech gadget. The result is that security must be planned over a longer period of time. For example, a requirement for more stringent cryptography, that is perhaps believed to be resistant to quantum attack, may be more important to deploy in a furnace sold in the near future, than a smartphone, as the smartphones are likely to be out of use in 2–3 years, while the furnace may have a 10 to 20 year lifecycle. Again, the longevity of these products and the implications for security are not easily signaled in the marketplace, and may require appropriate incentives or policy to help ensure the desired policy outcome of a secure and private IoT ecosystem.

¹⁰See, Husted and Myers, *Emergent Properties & Security: The Complexity of Security as a Science*, Proceedings of the 2014 New Security Paradigms Workshop (2014), pp. 1–14, Victoria, British Columbia, Canada, ACM.

Building from these steps, an overarching approach to enhancing the Security of Things may be promoted that considers IoT as an ecosystem, and encourages IoT providers to take responsibility for how their products impact the entire ecosystem (such as how a smart home interfaces with an autonomous vehicle). Entities that are information gatherers, information aggregators, and information transmitters/communicators, for example, could be liable for misusing user data, especially when such misuse has downstream consequences or involves critical or highly sensitive information.¹¹ Similarly, organizations that produce consumer products that enact poor physical outcomes, by interacting with users or their environments and produce damage while being used for their intended purpose, as deployed by a typical user (and not an expert), might be considered partially liable for such damages if their security posture did not meet some industry norms. The use of such an approach creates incentives for self-monitoring of the ecosystem and may encourage various industries across the IoT landscape to work together and gain a broader perspective on how IoT devices and data interact. The IoT ecosystem approach could help incentivize participants to develop and maintain an appropriate level of cybersecurity, is flexible to information type, and is malleable to changes in the environment, even as it insists upon ecosystem monitoring and taking accountability for the entirety of the system. Industry outliers could also find it difficult to purchase and/or share information with cooperative industry participants.

Moreover, lessons from related areas should not be ignored since device management issues that arise in IoT also come about within other analogous fields. Consider two recent examples: Google and Mattel. Turning to Google first, under the Family Educational Rights and Privacy Act (FERPA), a school needs to obtain written consent from parents before sharing personal information about students, except when the school sharing data with “school officials” have a “legitimate educational interest” in the data.¹² This definition has been interpreted to include contractors, since schools now outsource some of their functions.¹³ And, Google—it seems—falls under that definition.¹⁴ The result is that Google has been gathering a great deal of information about students as a result of their use of certain Google products such as Droid-powered tablets and has been using that information within its own ecosystem of GoogleWorld, with parents having no ability to prevent such information gathering.¹⁵ How Google will use, protect, and store this student information, how or with what data sources will this information be aggregated, and to whom will it pass on this information remain open questions as of this writing.

Mattel is another large corporate entity that has the ability to aggregate information across product lines and information sources. Yet, it seems unaware of the public’s growing awareness of the ‘creepy’ factor in the emerging IoT landscape. In 2015 Mattel released “Hello Barbie,” a smart doll that has a microphone and Wi-Fi connectivity that allows Mattel to host two-way conversations with children.¹⁶ And while one can assume the backlash was instant, in fact several privacy groups alerted individuals to the two-way communication feature in early 2015,¹⁷ yet the doll was released without major modification in time for Christmas 2015.¹⁸ This example serves as a reminder that industry self-monitoring can only serve as a mechanism to flag industry outliers; it cannot by itself change the behavior of multinational businesses that seek to take advantage of poorly constructed or antiquated policy, or individual user apathy. Consequently, while it is true that the desire for industry self-regulation seems justified given the still nascent state and rapid development of the underlying technologies, some IoT regulation may in fact be necessary, especially in critical areas of concern, such as transportation and healthcare. However, regulation should be limited to at-risk areas or populations (such as children) and should be crafted to reinforce existing best practice frameworks, as has

¹¹ See, e.g., Occupational Safety & Health Admin., <https://www.osha.gov/workers/index.html> (last visited Jan. 5, 2015).

¹² Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99, (1974).

¹³ See Department of Education, *Family Educational Rights and Privacy Act (FERPA)*, Final Rule, 34 CFR Part 99, 5 (2008) <http://www2.ed.gov/policy/gen/guid/fpco/pdf/ht12-17-08-att.pdf>.

¹⁴ See Andrea Peterson, *Google, A ‘School Official?’ This Regulatory Quirk Can Leave Parents In The Dark*, WASH. POST, (Dec. 30, 2015).

¹⁵ *Id.*

¹⁶ See Benjamin Snyder, *Activists Fight Release Of New High-Tech Barbie Doll From Mattel*, FORTUNE, (Mar. 25, 2015).

¹⁷ See Alejandro Alba, *Mattel’s Talking Hello Barbie Doll Raises Concern Over Children’s Privacy*, DAILY NEWS, (Mar. 16, 2015).

¹⁸ See *id.*

arguably happened in the electricity regulatory context.¹⁹ Most important to a self-regulatory model, policymakers must create incentives to encourage the further refinement of best practices as part of an ecosystem of information system participants.

In the creation of the IoT regulatory interventions, policymakers must recognize one important behavioral element; individuals often behave in a less than protective manner when it comes to what they share online. Consider Wyndham as an example; individuals continued to provide information to Wyndham after the breach was discovered but before litigation ensued. What should Wyndham (and others) take away from that fact? Unfortunately, one lesson is that people, in general, are often-times unwilling or incapable of protecting their own information, especially given the recent deluge of data breaches.²⁰ Yet consumers are at risk in data breaches, especially in the IoT environment, and that fact serves as an insulator to information security accountability. Thus, the ability to blame user error or to limit accountability for due diligence based on general use of service consent needs to be questioned. People are predictably apathetic when it comes to their online behavior, such as reading terms and conditions.²¹ As a result, businesses should accept some responsibility in protecting PII. For example, the Health Insurance Portability and Accountability Act (HIPAA) only covers patient information kept by health providers, insurers and data clearinghouses, as well as their business partners, but these definitions are vague. The result, in January of 2015 Jacqueline Stokes discovered the home paternity test results of 6,000 unsuspecting people openly available online.²² The individuals had consented to the use of the test, and had agreed to receive their results online, but had not consented (without ever reading the terms of use) to the information being used in aggregate for research and other search activities. As this example illustrates, policymakers need to create an information ecosystem that insists upon accountability while encouraging the reporting of data loss within a flexible regulatory model, while managers should be encouraged to plan for the likely behavior of users such as by designing automatic security and privacy opt-out protections. Similarly, policymakers should consider businesses responsibility to not only provide security and privacy features in their products, but to provide them in a manner that is “on by default” and easily understood by the average consumer—and not just technical experts. When wireless routers were initially being widely deployed throughout consumer households, they often came with many security features, but they were difficult and cumbersome to deploy. Laws at the state level requiring that manufacturers provide notice about wireless insecurity issues and to provide guidance on secure installation may have had an effect to prompt more user friendly and easy to manage security services.

Policymakers should also consider instances where the industry simply cannot make the decisions about what to do with a given type of information within the IoT ecosystem. For example, consider the case of a Florida woman’s car that informed authorities after she allegedly rear-ended two vehicles and left the scene without reporting the accident to the authorities.²³ In this instance, Ms. Bernstein had activated Ford’s Emergency Assistance safety feature after she was involved in a “sudden change of speed or movement.”²⁴ In these instances, the Emergency Assistance feature automatically places an emergency call to local first responders allowing emergency personnel to assist injured or otherwise incapacitated individuals. Unfortunately, Ms. Bernstein was neither and was instead allegedly intent on leaving the scene of the accident.²⁵ While this information may be detrimental to Ms. Bernstein—and those similarly situated as her—such information must not necessarily be shielded from sharing given that it serves a public good, in this case of promoting traffic safety and accountability. However, it is alternately easy to

¹⁹ See INTELLIGENCE & NAT’L SEC. ALLIANCE, ADDRESSING CYBER SECURITY THROUGH PUBLIC-PRIVATE PARTNERSHIP: AN ANALYSIS OF EXISTING MODELS 7 (Nov. 2009), www.insaonline.org/i/d/a/Resources/Addressing_Cyber_Security.aspx.

²⁰ See World’s Biggest Data Breaches, <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/> (last visited Jan. 5, 2015).

²¹ See Rebecca Smithers, *Terms and Conditions: Not Reading the Small Print can mean Big Problems*, GUARDIAN (May 11, 2011), <http://www.theguardian.com/money/2011/may/11/terms-conditions-small-print-big-problems>.

²² See Charles Ornstein, *Federal Privacy Law Lags Far Behind Personal-Health Technologies*, WASH. POST (Nov. 17, 2015). Unfortunately, the tail of the lost medical information is a tale often told. For example, in 2011 an Australian company did not properly secure details of hundreds of paternity and drug tests, making them accessible through a public Google search. *Id.*

²³ See Trevor Mogg, *Hit-And-Run Suspect Arrested After Her Own Car Calls Cops*, DIGITAL TRENDS, (Dec. 7, 2015).

²⁴ *Id.*

²⁵ *Id.*

imagine a future where ubiquitous sensor monitoring of data that is available for the public good results in an Orwellian state, and policy will be needed to find appropriate balances—such decisions almost surely should not be left to corporations.

It is also important to encourage effective cybersecurity workforce development including the necessity of baking in proactive cybersecurity best practices from the inception of a new IoT product line. The lesson here is constant vigilance, *e.g.*, letting an initial process of cybersecurity due diligence be the first, and not the last, word in an ongoing, comprehensive cybersecurity policy that promotes cyber hygiene along with the best practices essential for battling the multifaceted cyber threat.²⁶ Such a policy should be widely disseminated and regularly vetted as part of an overarching enterprise risk management process, along with having an incident response plan in place that includes private and public information sharing mechanisms.²⁷ These recommendations are in line with FTC guidance, as seen in the Wyndham settlement order, which should be considered the ground floor of compliance to be supplemented by the NIST Cybersecurity Framework and NIST IoT Framework to check for governance gaps that may then be filled in by industry best practices. Concrete steps for retailers, for example, in addition to the above could include installing software to deactivate RFID tags after a pre-determined period of time so as to avoid consumer privacy concerns. Powershelves could similarly limit real-time location tracking to only specific applications. Health data should be encrypted from end-to-end to help get ahead of the HIPAA–HITECH Act regulatory curve. Voluntary private-sector driven certification schemes could also be created to signal to customers as to those IoT companies that have taken such basic cybersecurity measures.²⁸

Globally, the U.S. Government should build on the progress made in cybersecurity norm building such as in the critical infrastructure context with a new focus on IoT. This is already happening to an extent in several cross-border partnerships have emerged that may present yet another option to protect sensitive PII. For example, in December 2010, the U.S. Department of Health and Human Services (HHS) and the European Commission’s DG CONNECT signed a Memorandum of Understanding (MoU) on Cooperation surrounding eHealth/Health IT.²⁹ The MoU was signed to demonstrate a shared dedication to strengthening transatlantic cooperation in eHealth and Health Information Technologies. In 2013, DG CONNECT and HHS published a first Roadmap of specific MoU actions.³⁰ Since then, this Roadmap has guided activities in two priority areas (work streams):

1. Standards development to advance the development and use of internationally recognized standards supporting transnational interoperability of electronic health information and communication technology, and
2. Workforce development to develop and expand the skilled Health IT workforce in Europe and the U.S.³¹

In 2015, it was agreed between DG CONNECT and the U.S. HHS to add a third priority area: Transatlantic eHealth/Health IT Innovation Ecosystems.³² This work stream aims to encourage innovation in the eHealth/Health IT industry and ensure linkages to the other two Roadmap work streams.³³ Over time, further linkages could be added to this and other IoT partnerships; indeed, the active collaboration surrounding the NIST Cybersecurity Framework could be extended with a special

²⁶ See GREGORY J. TOUHILL & JOSEPH TOUHILL, CYBERSECURITY FOR EXECUTIVES: A PRACTICAL GUIDE 291 (2014) (“You should measure your cybersecurity posture as part of your efforts to practice due care and due diligence, monitor and control your information systems, maintain legal and regulatory compliance, meet contractual obligations, and maintain certifications.”).

²⁷ For more on this topic, see Amanda N. Craig *et al.*, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 18 AM. BUS. L. J. 721 (2015).

²⁸ See David Inserra & Steven P. Bucci, *Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*, HERITAGE FOUND. (Mar. 6, 2014), <http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace>.

²⁹ EUROPA, MEMORANDUM OF UNDERSTANDING (2010), <http://ec.europa.eu/digital-agenda/en/news/memorandum-understanding-eu-us-ehealth>.

³⁰ EUROPA, TRANSATLANTIC EHEALTH/HEALTH IT COOPERATION ROADMAP (2013), <http://ec.europa.eu/digital-agenda/en/news/transatlantic-ehealthhealth-it-cooperation-roadmap>.

³¹ *Id.*

³² *Id.*

³³ Public Stakeholder Consultation on Next Phase of EU-US Cooperation in eHealth/Health IT, (Europa Press Release, Apr. 2015), <https://ec.europa.eu/digital-agenda/en/news/public-stakeholder-consultation-next-phase-eu-us-cooperation-ehealthhealth-it>.

emphasis on IoT concerns as part of the growing bottom-up approach to enhance the Security of Things.³⁴

Conclusion

We have come a long way since Kevin Ashton first used the expression “Internet of Things” as the title of a presentation he gave for Proctor & Gamble in 1999. The promise of networked smart devices is finally being realized, but in order to avoid the same litany of cyber attacks and data breaches we have seen in other contexts it is vital to adopt proactive policies that help drive the evolution of effective and secure IoT governance before cyber insecurity becomes replete in the Internet of Everything.

PREPARED STATEMENT OF LARRY CLINTON, PRESIDENT AND CEO,
INTERNET SECURITY ALLIANCE

Cybersecurity Is Not An “IT” Issue. To Address IT Effectively We Need To Look At Cybersecurity As An Economics Issue

Expecting technology to provide the answer to our cybersecurity problems would be a perilous course. A more promising path would be to understand the true nature of the cyber threat and take a more enterprise wide approach to addressing it.

Two months ago, the National Association of Corporate Directors (NACD) released the second edition of its Cyber-Risk Handbook, the only private sector cybersecurity document ever endorsed by both the departments of Homeland Security and Justice.

The very first principle of the NACD Cyber Risk Handbook is that cybersecurity is not an information technology issue. While it has a substantial technological component, cybersecurity is an enterprise-wide risk-management issue.

Information technology is only the pathway for cyberattacks—the “how” of cyberattacks.

If we are to address the cybersecurity issue in a long term, sustainable fashion we need to not only address the “how” of cybersecurity, but also the “why” of cybersecurity: the reasons that attacks occur.

From the private sector perspective, (and the core of the Commerce Committee’s jurisdiction) the reason cyberattacks continue to occur is the unbalanced nature of digital economics.

The basic equation of cybersecurity economics is this. Cyberattack methods are easy and cheap to access, they can generate enormous profits—in the hundreds of billions of dollars—and the business plan for the attackers is secure and sustainable as attackers reinvest in their enterprise to become ever more sophisticated and effective.

On the security side, cyber defense must protect an inherently insecure system that is growing technologically weaker with the explosion of mobile devices and the Internet of Things. We are almost inherently a generation behind the attackers, our laws and regulations are not well suited to address international and often state-sponsored digital threats. Moreover, the government mandates being piled on the private sector are often counterproductive. Finally, there is virtually no effective law enforcement. We successfully prosecute less than 2 percent of cyber criminals.

So long as we continue to try to address the cybersecurity issue from a technocentric perspective and ignore the fundamental economics that are driving the problem, we are destined to continue to fail badly.

To effectively address this issue, we must frame it differently. The problem is not that the technology is bad. Modern technology is nothing short of amazing.

The problem is that the technology is under attack. And the reason the technology is under attack is because all the economic incentives favor the attackers.

That is a fundamentally different problem that demands fundamentally different set of solutions. Within the private-sector, we have begun to address the issue in a broader risk management perspective that includes technology but places it in the context of the overall enterprise operation, not at the center of it. We are already seeing positive results.

For example, PricewaterhouseCoopers, in their 2016 Global Information Security Survey reported that “Guidelines from the National Association for Corporate Directors (NACD) advise that Boards should view cyber-risks from an enterprise-wide standpoint and understand the potential legal impacts. . . . Boards appear to be listening to this guidance. This year we saw a double-digit uptick in Board participation in most aspects of information security. Respondents said this deepening Board

³⁴ See Scott J. Shackelford, Scott Russell, & Jeffrey Haut, *Bottoms Up: A Comparison of “Voluntary” Cybersecurity Frameworks*, 16 UNIV. OF CAL. DAVIS BUS. L.J. 217 (2016).

involvement has helped improve cybersecurity practices in numerous ways. It may be no coincidence that, as more Boards participate in cybersecurity budget discussions, we saw a 24 percent boost in security spending.”

The Internet Security Alliance believes the Senate Commerce Committee, indeed the full Senate and Congress can help facilitate further progress by addressing the cybersecurity issue in a less techno—centric, and more enterprise risk management/economic fashion. ISA would offer three paths for the Commerce Committee to pursue.

Steps Toward Creating Better Economics For Cybersecurity

ISA would like to suggest three measures for improving cybersecurity that come within the jurisdiction of the Senate Commerce Committee.

1. Create a Rational Cyber Regulatory System
2. Promote incentives
3. Test the NIST Cybersecurity Framework for cost effectiveness.

Create a Rational Cyber Regulatory System

No one, certainly not ISA, is saying we ought not to have cyber controls or assessments. But we need to have a rational and well-thought out system or we will waste vital resources and undermine our security.

Earlier this week ISA released a “Cyber Regulation Fact Sheet.” The fact sheet (attached) demonstrates multiple examples of how the tremendous growth in cybersecurity rules and regulations is diverting scarce security resources and undermines our Nation’s cyber defenses.

One of the unintended consequences for organizations like ISA that has been raising awareness of the cyber threat for 15 years, is that we now have cyber mandates spring up like weeds as virtually every governmental entity, Federal state and local fight to be the “cyber guy.” The result is an uncoordinated, inconsistent and often counterproductive setoff requirements that is actually hurting, not helping, to increase security.

Research tells us we are experiencing more than a million cyber-attacks a year and we don’t have nearly enough cyber professionals to help protect us. We need to use our scarce resources efficiently and effectively. Yet some firms are now spending 30 percent of their budgets and 40 percent of their time of various compliance regimes none of which have been shown to empirically aid in securing our cyber systems.

ISA’s fact sheet offered numerous examples from multiple industry sectors of the growth on cyber regulations often inconsistent with the risk management philosophy that professionals overwhelmingly suggest is a more effective approach to cyber defense. Among the statistics cited are:

- In financial services increases of over 300 percent in cybersecurity and privacy related questions financial institutions now need to answer.
- In defense there are new rules for unclassified controlled information that force companies to label bits of information based on 23 categories, 84 sub-categories and hundreds of different citations. Ironically these rules could actually make it easier for attackers to find useful data.
- In Energy DOE has proposed requirements (10 CFR 73.53) that all networks in the sector meet controls (DG 5062) so overly broad that the mandate will require the expenditure of millions of dollars to implement controls not tailored for the risk of the networks.
- New defense acquisition rules will require small companies to comply with extraordinary detailed requirements that may well drive many smaller firms out of the defense business which is both inconsistent with DoD policy to promote the use of smaller companies but also harms national security as many of these firms are the top suppliers who can find markets for their services that don’t require the extensive compliance
- Various regulators are demanding public disclosure of supposedly material cyber-attacks when in fact the attack itself may not have a material effect, but the disclosure may well trigger unjustified (and usually temporary) stock fluctuations. As a result, it is the disclosure creating the material effect and provides a path for stock manipulation contrary to the regulator’s mission.

Our fact sheet is by no means an exhaustive list it is merely illustrative of the uncoordinated government response to the cybersecurity problem that need to be brought under control.

Part of this problem is that the government itself is not properly structured for the digital age and hence digital age issues like cybersecurity run into legislative and executive jurisdictional barriers. However, the Commerce Committee with its overarching mandate to promote U.S. commerce may well be positioned to provide some of the needed coordination.

Promote incentives

We believe that the most effective way for the private sector to improve the level of its cybersecurity is for the Congress and the Federal Government to consider what sets of incentives for better risk management can be brought to bear.

Government incentives allocated to the private sector in exchange for behaviors that, without incentives, would be not economically sustainable are not unprecedented. They are responsible for the telecommunications and electric infrastructure that undergird much of American prosperity. We call this the “social contract” approach to infrastructure and the Internet Security Alliance has long argued that a similar approach is needed for cybersecurity.

In the early twentieth century, the hot technologies of the time were telecommunications (phones) and distributed electricity. Initially these services were provided where the economies justified them: urban and affluent areas. The policy makers of the era not only understood that universal service of these technologies would have broad social benefit but also realized government couldn’t accomplish this on its own. Moreover, compelling the private sector to provide the services without adequate compensation would be an unsustainable model. So a “social contract”—essentially an economic deal—was developed. Private companies agreed to provide universal service at regulated rates. In exchange, the government agreed to guarantee a substantial rate of return on their investments.

And it worked. The broader systemic benefits of the social contract were enormous. The electric and telecommunications infrastructures were deployed at an accelerated pace compared with other nations that chose a government-centric model. Moreover, the infrastructures, adequately supported by the economic incentives imbedded in the contract, were continually made more sophisticated and innovative. The rapid development of these infrastructures provided the foundation for accelerated industrialization, job creation, and innovation. These systemic effects were essential to turning the United States from a second-rate world presence at the turn of the twentieth century into the world’s leading superpower in a little more than a generation.

More recently, the House GOP Task Force on Cybersecurity made their number one recommendation to develop a menu of incentives for the private sector to begin to address the economic incentive imbalance discussed above. To be fair there has been some progress since the House GOP report. In 2013 President Obama in his Executive Order 13636 also embraced the notion of using market incentives as opposed to regulatory mandates to promote cybersecurity and in the last Congress bipartisan legislation on cyber information sharing used the market incentive of liability protection.

As we move forward we need to enhance and accelerate the development of market incentives. While obvious techniques such as tax breaks for smaller companies to adopt sophisticated defenses not otherwise commercially justifiable can be used, there are many other models of incentives that can be adapted. For example, just as pharmaceutical companies with good records can gain access to an accelerated drug approval process perhaps good actors in technology could get patent approval preference, or utilities could gain access to a fast rerack permitting system. Regulatory forbearance could be offered for organizations meeting specified levels of maturity in traditionally regulated industries and streamlined audit and assessment process can also be developed.

The reality is that many cyber-attacks are nation-state backed and no private organization can match the resources of a nation state. It may well be that private companies will have to take on traditionally governmental responsibilities in the digital age and government needs to find a sustainable and cost efficient mechanism to deal with this new reality.

No less a source than the National Infrastructure Protection Plan (NIPP) has observed that the private sector and the public sector assess cyber risk on very different dimensions. For the private sector—operating under a mandate to maximize shareholder value—the cybersecurity calculus is largely economic. This reality generates a higher level of security risk tolerance in the private sector than the public sector. For example, a private entity maybe comfortable with allowing 10 percent of inventory to “walk out the back door” every month because it will cost 11 percent to purchase the additional guards and cameras to fully secure themselves. The pub-

lic sector doesn't have this luxury. Government has enormous non-economic concerns it must accommodate such national security and citizen privacy.

Today, we need a twenty-first-century systems approach to address the cybersecurity issue. The new model needs a much more dynamic motivator than backward-looking regulations and potential enforcement. Since 90 percent of infrastructure is owned and operated by the private sector and the principal problem with cybersecurity is economic, the best model to promote a forward-thinking risk-management approach to cybersecurity would be injecting positive economic incentives into continual upgrading and management of private cyber systems.

Test the NIST Cybersecurity Framework for cost effectiveness.

The NIST Cybersecurity Framework rightly enjoys the praise of wide swaths of government and the private sector. We join in that praise, although we note that the Framework is not a standard but a broad framework that can, and ought to be, implemented in many ways depending on unique aspects of the system its being applied to and the threats that system is facing. As such, the specific way the Framework is used is not necessarily the most cost effective approach. This is why the executive order that called for the Framework's creation, E.O. 13636, also stipulates that the Framework ought to be *cost effective*—a direct call to address the economic imbalance causing the cybersecurity crisis.

Unfortunately, three years after NIST released the Framework, there have been no efforts to evaluate it for cost effectiveness.

This is even despite Section 104 (b) of the recently signed American Innovation and Competitiveness Act, which in states that NIST shall “conduct research and analysis (A) to determine the nature and extent of information security vulnerabilities and techniques for providing *cost effective information security*” (emphasis added).

The lack of data in this area is a huge drag on cybersecurity since the commercial sector cannot afford economically unsustainable cybersecurity measures. It's likely led to an underinvestment in cybersecurity in many sectors, since it's impossible for companies to trace the quantitative reduction in risk exposure caused by cybersecurity measures.

Most importantly, lack of cost data makes it impossible for the government to understand which specific areas of cybersecurity it should spend its considerable powers on encouraging within the private sector. In the absence of data, cybersecurity advice tends toward the general, along the lines of “implement best practices.” But abstract exhortation is not working. We now need to know *which* best practices, and *why* they're not being adopted. The ISA suspects cost is a major factor.

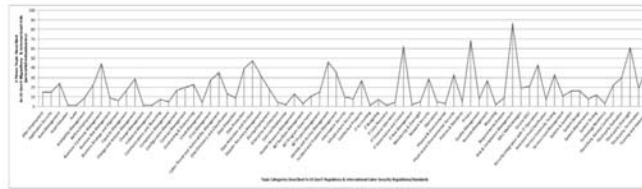
After determining cost effectiveness, the government should move to create incentives to encourage adoption. Steps that improve the bottom line by diminishing quantifiable risk will find natural take up by the private sector. But measures that are effective but too expensive to justify economically—but necessary for securing the economic and national security of the United States—are precisely where targeted incentives should be deployed.

We urge the Committee ought to use its tools and processes to test the cost effectiveness of NIST Framework implementation.



Cyber Regulation Fact Sheet

- Estimates of approximately 1.5 million cyber-attacks each year.
- Experts estimate we have a shortfall of about 1.5 million qualified cybersecurity professionals.
- Forty-five percent of organizations say they have a problem filling their cybersecurity needs.
- From 2012-2015, financial institutions noticed over a 300% increase in the number of cybersecurity and privacy related questions they must answer for compliance purposes.
- Some firms' Chief Information Security Officers report spending almost 40% of their time just on compliance measures and audits.
- Some firms now spend 30% of their cybersecurity budgets on compliance. More than sixty (60) various security standards/frameworks exist, just for financial institutions.



- The chart above depicts the number of times each of 73 listed security related categories are addressed (not just mentioned) in the US government & international cybersecurity regulations/standards being tracked by financial services companies.
 - The Risk & Compliance Management topic (tallest) peaks at just under 90 authoritative sources, meaning it's addressed somehow in 90 out of the 332 US relevant cyber regulations being tracked.
 - Sixty-seven of the 73 topic categories have redundant authoritative sources.
- Thanks to investment from major defense firms, the DIB suffers 1/3 less successful cyber-attacks than other industry sectors. However, application of procedures that require organizations to apply the security controls of NIST SP 800-171, designed for large defense contractors, to the many small companies in the supply chain is counterproductive. For example:
 - The Defense Federal Acquisition Regulation Supplement (DFARS) rule, which requires organizations to apply the security controls of NIST SP 800-171, is not in keeping with a risk management approach to cybersecurity. It demands enormous check the box compliance processes for smaller players on controls that have little to do with combating the types of threat most dangerous to defense systems and diverts scarce resources from controls required to address the most serious threats. Some of the most exploited methods used against the

defense supply chain aren't addressed. The unnecessary compliance procedures are a disincentivization for critical smaller players to participate in defense contracting. This conflicts with DoD goals of increasing participation of smaller players, and deprives our systems of access to the best and most innovative providers for critical elements needed to build the best defense systems. Moreover, the binary "pass-fail" process for assessing compliance fails to appropriately reward smaller players for the cost-efficient improvements they may make, which might well be sufficient to provide adequate security given their specific role in the supply chain.

- On a contract by contract basis, departments are inserting ad hoc cybersecurity controls exceeding those promulgated by NIST. This creates excessive compliance overhead with minimal impact to risk reduction. A uniform standard of risk based security should be agreed upon for the protection of data at pre-determined classification levels across all departments and agencies.
- The September 2016 final rules implementing a November 2010 Executive Order 13556 on Controlled Unclassified Information (CUI). Since 2010, the information technology world has evolved considerably, yet the final rule is deeply rooted in the analog world of 2010. The new rule contains no less than 23 categories of CUI, 84 sub-categories, and several hundred citations. This approach wastes time and effort of the individuals who are concerned with marking CUI, and diverts time and money from the critical nature of what EO 13556 was trying to achieve - *protecting the information*. The new rule compromises security.
 - For example, using the current ruling, unclassified nuclear information would be marked "CONTROLLED/Nuclear – Unclassified Controlled Nuclear Information – Defense", one of the 84 sub-categories. This identification provides a virtual roadmap for any foreign actor who is attempting to steal critical information from a federal or contractor network. A more sensible approach would be to simply mark CUI as CUI. It makes the digital protection of the information much less complex, allowing federal contractors to worry more about the protection of the information than which of the 84 sub-categories they should use in marking the data. The CUI rules will have a significant impact to the cost of compliance with little impact on risk reduction.
- The SEC requires disclosure of material information regarding cyber risks and incidents. These requirements may be appropriate for investor confidence in businesses highly dependent on their network posture such as on-line retailers or financial institutions. However, for other sectors, e.g. manufacturing, a breach may not be inherently financially material until it is disclosed, at which point stock prices may suffer a short-term negative impact (research demonstrates the stocks almost universally rebound—often increasing). However, the mandatory disclosure creates a vehicle for stock manipulation – a growing area of cybercrime – with no actual material damage from the cyber breach, other than that caused by the disclosure.
- One size does not fit all. All data in a sector is not equal, nor do all networks in a sector connect to Vital Digital Assets. The Department of Energy, Nuclear Regulatory Commission has proposed requirements (10 CFR 73.53) that all networks in the sector meet controls (DG 5062) written to protect VDAs. The overly broad mandate will require the expenditure of millions of dollars to implement controls not tailored for the risk of the networks.
- None of the above rules and regulations have been empirically shown to improve actual security.

PREPARED STATEMENT OF THERESA PAYTON, CEO, FORTALICE SOLUTIONS LLC

Chairman Thune, Ranking Member Nelson, distinguished members of the Committee:

It is an honor to submit this written testimony on behalf of Fortalice Solutions LLC (“Fortalice”). Fortalice is a cybersecurity and intelligence firm that provides and enhances national and economic security through the delivery of highly-focused, mission-critical cybersecurity solutions to top business and government entities. We are a team of cybercrime fighters, techies, geeks, policy wonks, and enthusiastic security and intelligence professionals, who strive to protect people, businesses, and nations against threats to their cyber footprint. Fortalice applauds the Committee for prioritizing cybersecurity and focusing on how the Nation can most effectively achieve the equally important goals of: (a) unleashing rapid, continued technological innovation, and (b) ensuring that technology is secure. Many in private industry and the government argue that achieving these goals requires a balancing act. Focusing on a solution that seeks to balance these goals, however, does a disservice to the nation: a balancing act insinuates that both sides of the equation—innovation and security—must give a little to achieve balance. Fortalice believes private industry and government need to move toward an integrated risk philosophy that accelerates and *maximizes*, not balances, innovation and security.

Explosion of Emerging Technologies and Challenges

A few years ago when Ted Claypoole and I wrote our second book on Internet privacy and security, “Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family,” we predicted that the broken technology innovation lifecycle, combined with outdated security strategies, would be overrun by consumers’ insatiable desire to rapidly integrate the latest digital advancements in apps, social media platforms, and smart devices at home and at work. We predicted this would create a security and privacy conundrum by 2020, but that prediction came sooner than we anticipated.

In the Internet of Things (IoT) area alone, the predictions for the explosion of emerging technologies are staggering. Gartner predicts that by the end of this year, 8.4 billion “things” will be connected, a 31 percent increase from 2016, and that by 2020 we will reach 20.4 billion connected “things.”¹ Internet connected refrigerators have long been the poster child of IoT.

Recent events indicate that there is more to it than just worrying about your home refrigerator spilling your dieting secrets to the world. This explosion in digital devices, the data they collect, and the integration into our every day workplaces and personal lives, provides numerous economic and societal benefits—but it will also require the security marketplace and practitioners to immediately change the paradigm they use to design security solutions to one that enhances security products and services. We cannot take a pause on innovation to integrate security. IoT creates new business value, improves customer experiences, and may possibly even save lives. For example, in the U.K., neighborhoods are testing an IoT street lamp that shines extra-bright when it detects noises such as banging and hollering. It’s also armed with cameras that transmit a live video feed to the cloud for further review.

Despite its wonderful impact on our lives, emerging technology creates more complexity for security teams because of lagging security approaches and infrastructure. The security company, RSA, released a Cyber Security Poverty Index in 2016 that indicated that 72 percent of large enterprises, and these are the ones with the budget and resources for a robust security program, are unprepared for all aspects of a data breach (including identifying the scope, recovery, and notification).²

Why do we need to act now? Security issues existed well before integrating emerging technology, including IoT. Candidly, if we do not make a commitment to a major shift in how we establish a new set of security protocols, human safety, not just data, is at risk. How many warnings do we need before we act? Many U.S. adults report they have had their data reported stolen in a data breach and, in some cases, have been victimized by identity theft. In fact, 2 in 5 Americans reported to Bankrate.com that they have either been an identity theft victim or know someone who has—this is a staggering statistic that continues to escalate.³ We also know

¹Gartner. Press Release, “Gartner Says 8.4 Billion Connected “Things” Will Be in Use in 2017, Up 31 Percent From 2016.” February 7, 2017.

²RSA. “2016 RSA Cybersecurity Poverty Index.”

³Dickler, Jessica. “41 Million Americans Have Had Their Identities Stolen, Survey Finds.” CNBC. October 11, 2016.

from recent FBI reports that intellectual property theft, ransomware, and extortionware are on the rise. As seen in October 2016, random cybercriminal groups can impact major companies like Amazon, Twitter, and Netflix, who are almost solely dependent upon the reliability of the web, and render them unavailable to their customers via a Distributed Denial of Service (DDoS) attack. We must not wait to change how we protect and defend our emerging technology, data, and infrastructure until the next catastrophic attack impacts human safety. The safety of humans trumps cyber security. The time to act is now.

Fortalice believes there are several specific challenges overall for the security industry that this Committee should consider:

- *Marketplace demands for technological innovation are outpacing security:* An age old problem in the security industry is the technology innovation lifecycle. For far too long, industry has followed an inherently broken process for producing new products. First, the great thinkers on the innovation and design teams come up with an idea for the marketplace. Second, the innovation and design teams develop and build the product. Finally, once the product is already built, the innovation and design teams consult the security team during the testing phase. The security team may find vulnerabilities, however, it is often too late or too expensive to fix those vulnerabilities before going to market. Cybercriminals know this technology innovation lifecycle is flawed and take full advantage of it. Tomorrow's hot new IoT item is today's target of cybercriminals. This flawed lifecycle is exacerbated as emerging technologies hit the marketplace at a dizzying pace. As we saw in the DDoS attack on October 21, 2016, when the Internet screeched to a slow crawl and in some cases was inoperable, the lack of security in our emerging technology hit critical mass. On that fateful day, baby cams, smart devices from thermostats to security surveillance cameras, and numerous IoT devices were weaponized and used to target an Internet infrastructure company, Dyn. Dyn houses a portion of the web's domain name system (DNS) infrastructure. Companies, including but not limited to, CNN, Spotify, Reddit, the New York Times, Netflix, Amazon, and Twitter were all impacted that day. The DDoS attack was largely powered by the Mirai botnet which took over the unsecured devices of innocent consumers and businesses. This attack is considered the largest DDoS attack ever to be reported.⁴ How do we prevent another October 21st? The design phase must include security engineers at the beginning. Implemented correctly, elegant security design can enhance and improve the development cycle, contribute to speed to market, and create a market differentiator by focusing on privacy and security in the design.
- *Security marketplace often solves for past cybercriminal behavior and does not anticipate new tactics:* Security vendors today provide critical services that help companies monitor networks; these services are necessary but not nearly sufficient for combatting dynamic cybersecurity threats. While having coffee with my esteemed security colleagues recently, one challenged all of us to name a single security problem that has been 100 percent eliminated in the last decade by security solutions. We couldn't. The focus has been too heavy on minimizing risk, and as we saw when we hit a milestone of one million new pieces of malware released daily in 2015,⁵ it is challenging for the security industry to keep up. The best that most legacy security services model can do is react. For example, most security services scan for known vulnerabilities and then layer on more rules and more tools to protect against known vulnerabilities. While this is an important service, the security industry must also proactively anticipate the next wave of threats. We know something is wrong with our cybersecurity approach when worldwide spending on cybersecurity is predicted to top \$1 trillion for the five-year period from 2017 to 2021 and the Global Cost of Cybercrime will hit \$6 Trillion Annually in 2021.⁶ That is not a winning business case. The emerging technology lifecycle and the legacy approaches to security must be disrupted now.
- *NIST Framework sets a floor:* In 2014, this Committee spearheaded the Rockefeller-Thune act and significantly advanced cybersecurity by codifying a voluntary and risk-based process that forms the basis of major aspects of today's cybersecurity risk management landscape. Fortalice has performed dozens of as-

⁴ Woolf, Nicky. "DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say." The Guardian News and Media. October 26, 2016.

⁵ Harrison, Virginia and Pagliery, Jose. "Nearly 1 Million New Malware Threats Released Every Day." @CNNTech, April 14, 2015.

⁶ "Global Cost of Cybercrime Predicted to Hit \$6 Trillion Annually By 2021, Study Says." Dark Reading. October 26, 2017.

assessments against the resulting National Institute of Standards and Technology (NIST) Cybersecurity Framework, and as we've seen through our clients, the next phase for the NIST Framework should be enabling companies to develop functional plans of execution. In our work with private sector companies large and small, many are familiar with the NIST Framework and have performed the assessment, but they are unclear on how to integrate lessons learned from these assessments into their every day business processes.

A Framework for Maximizing Innovation and Security

Fortalice offers the following framework for maximizing innovation and security:

1. *Incentivize Security:* One reason security is broken for all of us is that security is not designed for the human psyche. We do not expect untrained consumers to do their own dental work or health physicals, but we expect them to know how to protect themselves online. This is a fundamental design flaw that needs to be changed through incentives. For companies that invest in cybersecurity, either as a buyer or developer of emerging technologies, offer R&D Tax Credits. For designers of emerging technology, this will provide the financial incentive to speed up and prioritize security engineering in design. For businesses purchasing emerging technology, the R&D tax credit for implementing security will incent them to ask the right questions of vendors and product manufacturers. The questions will lead to further adoption of best practices such as the NIST framework. Financially incentivizing security ensures it becomes a priority in the Boardroom in addition to the server room. Additional tax or financial incentives should be awarded to Internet Service Providers (ISPs) that agree to make security for businesses and consumers work "like an app". Imagine if businesses and consumers could update ISP routers with vital security patches, block known bad traffic, and receive alerts and warnings that Internet traffic is suspicious and have the option to block it all via an app. That is how you design for the human instead of asking the human to conform to security.
2. *Change the Narrative Regarding Data Breaches:* The more we know about a data breach, the more information we have to improve security designs. Recognize that all companies that are victims of cybercrime are truly victims. The media often vilifies companies that have a data breach. This creates a huge disincentive to companies that would otherwise come forward to share their lessons learned from data breaches when they are not compelled to do so.
3. *Make Emerging Technologies Work for Security:* Innovation and emerging technologies can be leveraged to accelerate security. For instance, IoT devices can be configured to produce behavioral based analytics and monitor critical assets. IoT security applications can also develop baselines for alerts and notify security practitioners of key indicators, such as when traffic volumes are high or when behavior patterns just don't make sense. Policies should be crafted to further this end.
4. *Promoting Risk Management Frameworks:* Perhaps the most important work that the Committee and Congress can do is to continue leveraging the legislative process to examine and assess the Nation's cybersecurity needs in the short- and long-term and ultimately seek enactment of smart legislative solutions. Fortalice commends the Committee on Rockefeller-Thune, and codifying the NIST Framework process, and urges the Committee to consider follow-on actions for this important legislation, such as codifying incentives to promote further adoption of risk-based cybersecurity models. Furthermore, private industry would benefit from help with implementation in the form of case studies with suggested implementation plans mapping out suggested first, second, and third technical steps to help them implement or transform their security programs. The Committee could go even further—work to shift the emphasis in future frameworks to making sure the basics are covered by providing industry benchmarks that help explain how an organization is protecting their data from the inevitable data breach.
5. *Communication and Awareness:* We encourage the Committee to develop a communication campaign leveraging case studies to continue to drive awareness. Examples include actively promoting the work of this Committee through conferences, social media sites such as LinkedIn, and opinion pieces in local and national newspapers.

About Fortalice Solutions

Fortalice Solutions was founded in 2009 by former White House Chief Information Officer, Theresa Payton, to provide and enhance national and economic security through the delivery of highly-focused, mission-critical cyber security solutions to

clients. She and her business partner, Vince Crisler, a former United States Air Force officer, former White House Communications Agency Presidential Communications Officer, and current cybersecurity subject matter expert to Fortune 200 companies, strive to ensure that every service and solution is grounded in practicality and a real-world understanding of the threats to people, their business, and nation. The Fortalice team represents the highest quality of cyber security and intelligence talent available today, and delivers analysis, training, action, transparency and creative problem solving to keep what matters most safe. Fortalice has deep experience in the cybersecurity life cycle, from the keyboards in the server room to the boardroom.

Fortalice services include:

- Designing, Protecting, and Orchestrating Significant National Security Events
- Risk, Threat, and Vulnerability Assessments
- Incident Response and Forensics Support
- Adversarial Targeting through Red Teaming and Penetration Testing
- Payment Card Industry (PCI), HITECH, FFIEC and Other Regulatory Compliance Support
- Cybersecurity Crisis Communications and Public Relations
- Business Protection Plans
- Strategic Spend Plan for Security that Answers: “How Much is “Enough”?”
- Confidential and Sensitive Company & Personal Communication & Data Protection Strategies
- Digital surveillance including Cyber asset and data protection for executives, high-net worth individuals, high-profile individuals (*e.g.*, politicians and celebrities), and victims of cyberstalking, revenge porn, and other cybercrimes
- Vendor Management and Supply Chain Security Protection

For more information visit us at: www.fortalicesolutions.com

The CHAIRMAN. We'll keep the record open for a couple of weeks so if senators have additional questions that they want to submit for the record. If you would respond as quickly as you can to those questions, we'll try and wrap it up within a couple of weeks time. So we would appreciate you doing that.

It has been a great panel. Thanks so much for your input. A lot of good interaction. Lots of questions, probably more questions than answers, but I think this is an issue that's going to be with us for some time, and it's important that we stay ahead of our adversaries and that we're constantly looking for new and better ways, not only of taking full advantage of the wonderful benefits of the innovation, the technologies out there, but also to make sure that we are securing and providing the right levels of security and safety for the American people and for users of these great systems.

So thanks again. We appreciate it, panel. And with that, this hearing is adjourned.

[Whereupon, at 12:15 p.m., the hearing was adjourned.]

A P P E N D I X

ELECTRONIC PRIVACY INFORMATION CENTER
Washington, DC, March 22, 2017

Hon. JOHN THUNE, Chairman,
Hon. BILL NELSON, Ranking Member,
U.S. Senate Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Chairman Thune and Ranking Member Nelson:

We write to you regarding the Committee's hearing on "The Promises and Perils of Emerging Technologies for Cybersecurity."¹ American consumers face unprecedented privacy and security threats. The unregulated collection of personal data and the growth of the Internet of Things has led to staggering increases in identity theft, security breaches, and financial fraud in the United States. Artificial Intelligence implicates a wide range of economic, social, and political issues in the United States. These issues have a significant impact on the future of cybersecurity, and we commend the Committee for exploring them.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.² EPIC is a leading advocate for consumer privacy and has appeared before this Committee on several occasions.³ EPIC is also focused on the impact of Artificial Intelligence (AI) on American society. In recent years, EPIC has opposed government use of "risk-based" profiling,⁴ brought attention to the use of proprietary techniques for criminal justice determinations,⁵ and litigated several cases on the front lines of AI. In 2014, EPIC sued the U.S. Customs and Border Protection under the Freedom of Information Act ("FOIA") for documents about the use of secret tools to assign "risk assessments" to U.S. citizens.⁶ EPIC also sued the Department of Homeland Security seeking documents related to a program that assesses "physiological and behavioral signals" to an individual's likelihood commit a crime.⁷

¹*The Promises and Perils of Emerging Technologies for Cybersecurity*, 115th Cong. (2017), S. Comm. on Commerce, Science, and Transportation, <http://www.commerce.senate.gov/public/index.cfm/hearings?ID=E0E0BBA1-231C-42A4-AF33-FC4DDDFCF43C3> (March 22, 2017).

²See EPIC, *About EPIC*, <https://epic.org/epic/about.html>.

³See, e.g., Marc Rotenberg, EPIC Executive Director, Testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, Commerce Committee, *Internet Privacy and Profiling* (June 13, 2000), <https://epic.org/privacy/internet/senate-testimony.html>; Letter from EPIC to the U.S. Senate Committee on Commerce, Science, and Transportation on Oversight of the FTC (Sept. 26, 2016), <https://epic.org/privacy/consumer/EPIC-Letter-Sen-Comm-CST-FTC-Oversight.pdf>; Letter from EPIC to the U.S. House of Representatives Committee on Energy and Commerce on FCC Privacy Rules (June 13, 2016), <https://epic.org/privacy/consumer/EPIC-FCC-Privacy-Rules.pdf>.

⁴EPIC *et al.*, *Comments Urging the Department of Homeland Security To (A) Suspend the "Automated Targeting System" As Applied To Individuals, Or In the Alternative, (B) Fully Apply All Privacy Act Safeguards To Any Person Subject To the Automated Targeting System* (Dec. 4, 2006), available at http://epic.org/privacy/pdf/ats_comments.pdf; EPIC, *Comments on Automated Targeting System Notice of Privacy Act System of Records and Notice of Proposed Rulemaking*, Docket Nos. DHS-2007-0042 and DHS-2007-0043 (Sept. 5, 2007), available at http://epic.org/privacy/travel/ats/epic_090507.pdf. See also, *Automated Targeting System*, EPIC, <https://epic.org/privacy/travel/ats/>.

⁵EPIC *Sues Justice Department Over "Risk Assessment" Techniques*, EPIC (March 7, 2017), <https://epic.org/2017/03/epic-sues-justice-department-o.html> (EPIC's Complaint against the DOJ is available at <https://epic.org/foia/doj/criminal-justice-algorithms/EPIC-v-DOJ-criminal-justice-algorithmscomplaint.pdf>).

⁶EPIC *v.* CBP (*Analytical Framework for Intelligence*), EPIC, <https://epic.org/foia/dhs/cbp/afi/>.

⁷EPIC *v.* DHS—FAST Program, EPIC, <https://epic.org/foia/dhs/fast/>.

The Internet of Things Poses Numerous Privacy and Security Risks

The Internet of Things (IoT) poses significant privacy and security risks to American consumers.⁸ The Internet of Things expands the ubiquitous collection of consumer data. This vast quantity of data could be used for purposes that are adverse to consumers, including remote surveillance. Smart devices also reveal a wealth of personal information about consumers, which companies may attempt to exploit by using it to target advertising or selling it directly. Because the IoT generates data from all aspects of consumers' daily existence, these types of secondary uses could lead to the commercialization of intimate segments of consumers' lives.

Many IoT devices feature "always on" tracking technology that surreptitiously records consumers' private conversations in their homes.⁹ These "always on" devices raise numerous privacy concerns, including whether consumers have granted informed consent to this form of tracking. Even if the owner of an "always on" device has consented to constant, surreptitious tracking, a visitor to their home may not. Companies say that the devices rely on key words, but to detect those words, the devices must always be listening. And the key words are easily triggered. For example, several Amazon Echo devices treated a radio broadcast about the device as commands.¹⁰ A San Diego television report about a girl using an Echo to order a \$170 dollhouse and four pounds of sugar cookies triggered Echo devices across the city to make the same purchase.¹¹ A recent law enforcement request for Amazon Echo recordings¹² shows that "always on" devices will be much sought-after sources of information by law enforcement, foreign and domestic intelligence agencies, and, inevitably, cybercriminals.

Another significant risk to consumers in the IoT is security, of both the users' data and their physical person. Many of the same security risks that currently threaten our data will only expand in the Internet of Things. The damage caused by malware, phishing, spam, and viruses will have an increasingly large array of networks in which to spread.¹³ Additionally, not all wireless connections in the IoT are encrypted.¹⁴ Researchers who studied encryption within the IoT found that "many of the devices exchanged personal or private information with servers on the Internet in the clear, completely unencrypted."¹⁵

In addition to data security risks, the IoT also poses risks to physical safety and personal property. This is particularly true given that the constant flow of data so easily delineates sensitive behavior patterns, and flows over networks that are not always secure, leaving consumers vulnerable to malicious hackers. For instance, a hacker could monitor Smart Grid power usage to determine when a consumer is at work, facilitating burglary, unauthorized entry, or worse. Researchers have already demonstrated the ability to hack into connected cars and control their operation, which poses potentially catastrophic risks to the public.¹⁶

It is not only the owners of IoT devices who suffer from the devices' poor security. The IoT has become a "botnet of things"—a massive network of compromised web cameras, digital video recorders, home routers, and other "smart devices" controlled

⁸ See Comments of EPIC to NTIA, *On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (June 2, 2016), <https://epic.org/apa/comments/EPIC-NTIA-on-IOT.pdf>; Internet of Things, EPIC, <https://epic.org/privacy/internet/iot/>.

⁹ EPIC Letter to DOJ Attorney General Loretta Lynch, FTC Chairwoman Edith Ramirez on "Always On" Devices (July 10, 2015), <https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf>.

¹⁰ Rachel Martin, *Listen Up: Your AI Assistant Goes Crazy For NPR Too*, NPR (Mar. 6, 2016), <http://www.npr.org/2016/03/06/469383361/listen-up-your-ai-assistant-goes-crazy-for-npr-too>.

¹¹ Carlos Correa, *News Anchor Sets off Alexa Devices Around San Diego Ordering Unwanted Dollhouses*, CW6 (Jan. 5, 2017), <http://www.cw6sandiego.com/news-anchor-sets-off-alexa-devices-around-san-diego-ordering-unwanted-dollhouses/>.

¹² See Christopher Mele, *Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concerns*, N.Y. Times (Dec. 28, 2016), <https://www.nytimes.com/2016/12/28/business/amazon-echo-murder-case-arkansas.html>.

¹³ See EUROPEAN COMM'n, A DIGITAL AGENDA FOR EUROPE, 16–18 (2010), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF>.

¹⁴ Federal Motor Vehicle Safety Standards; Event Data Recorders, Docket No. NHTSA–2012–0177 (Comments of Privacy Coalition), 10 <https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf>.

¹⁵ Nick Feamster, *Who Will Secure the Internet of Things?*, FREEDOM TO TINKER (Jan. 19, 2016) <https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-internet-of-things/> (emphasis in original).

¹⁶ See, e.g., Karl Brauer & Akshay Anand, *Braking the Connected Car: The Future of Vehicle Vulnerabilities*, RSA Conference 2016, https://www.rsaconference.com/writable/presentations/file_upload/ht-t11-hacking-the-connected-car-the-future-of-vehicle-vulnerabilities.pdf; FireEye, *Connected Cars: The Open Road for Hackers* (2016), <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/connected-cars-the-open-road-for-hackers.pdf>.

by cybercriminals who use the botnet to take down websites by overwhelming the sites with traffic from compromised devices.¹⁷ The IoT was largely to blame for attacks in 2016 that knocked Twitter, Paypal, Reddit, Pinterest, and other popular websites off of the web for most of a day.¹⁸ They were also behind the attack on security blogger Brian Krebs' website, one of the largest attacks ever seen.¹⁹

These problems will not be solved by the market. Because poor IoT security is something that primarily affects other people, neither the manufacturers nor the owners of those devices have any incentive to fix weak security. Compromised devices still work fine, so most owners of devices that have been pulled into the "botnet of things" had no idea that their IP cameras,

DVRs, and home routers are no longer under their own control. As Bruce Schneier said in recent congressional testimony, a manufacturer who puts a sticker on the box that says "This device costs \$20 more and is 30 percent less likely to annoy people you don't know" probably will not get many sales.²⁰ We urge the Committee to address these numerous privacy and security concerns as it moves forward on legislation related to the Internet of Things.

The Challenge of AI

There is understandable enthusiasm about new techniques that promise medical breakthroughs, more efficient services, and new scientific outcomes. But there is also reason for caution. Computer scientist Joseph Weizenbaum famously illustrated the limitations of AI in the 1960s with the development of the Eliza program. The program extracted key phrases and mimicked human dialogue in the manner of non-directional psychotherapy. The user might enter, "I do not feel well today," to which the program would respond, "Why do you not feel well today?" Weizenbaum later argued in *Computer Power and Human Reason* that computers would likely gain enormous computational power but should not replace people because they lack such human qualities and compassion and wisdom.²¹

We face a similar reality today. EPIC has concluded that one of the primary public policy goals for AI must be "Algorithmic Transparency."²²

The Need for Algorithmic Transparency

Democratic governance is built on principles of procedural fairness and transparency. And accountability is key to decision making. We must know the basis of decisions, whether right or wrong. But as decisions are automated, and we increasingly delegate decisionmaking to techniques we do not fully understand, processes become more opaque and less accountable. It is therefore imperative that algorithmic process be open, provable, and accountable. Arguments that algorithmic transparency is impossible or "too complex" are not reassuring. We must commit to this goal.

It is becoming increasingly clear that Congress must regulate AI to ensure accountability and transparency:

- Algorithms are often used to make adverse decisions about people. Algorithms deny people educational opportunities, employment, housing, insurance, and credit.²³ Many of these decisions are entirely opaque, leaving individuals to wonder whether the decisions were accurate, fair, or even about them.
- Secret algorithms are deployed in the criminal justice system to assess forensic evidence, determine sentences, to even decide guilt or innocence.²⁴ Several states use proprietary commercial systems, not subject to open government laws, to determine guilt or innocence. The Model Penal Code recommends the implementation of recidivism-based actuarial instruments in sentencing guide-

¹⁷See Bruce Schneier, *We Need to Save the Internet from the Internet of Things*, Schneier on Security (Oct. 6, 2016), https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html

¹⁸See Scott Hilton, *Dyn Analysis Summary of Friday October 21 Attack*, Dyn.com (Oct. 26, 2016), <http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>.

¹⁹See Brian Krebs, *KrebsOnSecurity Hit With Record DDoS*, KrebsOnSecurity (Sept. 21, 2016), <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>.

²⁰Testimony of Bruce Schneier before the House Committee on Energy & Commerce, *Understanding the Role of Connected Devices in Recent Cyber Attacks*, 114th Cong. (2016).

²¹Joseph Weizenbaum, *Computer Power and Human Reason: From Judgment to Calculation* (1976).

²²*Algorithmic Transparency*, EPIC, <https://epic.org/algorithmic-transparency/>.

²³Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).

²⁴*EPIC v. DOJ (Criminal Justice Algorithms)*, EPIC, <https://epic.org/foia/doj/criminal-justice-algorithms/>; *Algorithms in the Criminal Justice System*, EPIC, <https://epic.org/algorithmic-transparency/crim-justice/>.

lines.²⁵ But these systems, which defendants have no way to challenge are racially biased, unaccountable, and unreliable for forecasting violent crime.²⁶

- Algorithms are used for social control. China's Communist Party is deploying a "social credit" system that assigns to each person government-determined favorability rating. "Infractions such as fare cheating, jaywalking, and violating family-planning rules" would affect a person's rating.²⁷ Low ratings are also assigned to those who frequent disfavored websites or socialize with others who have low ratings. Citizens with low ratings will have trouble getting loans or government services. Citizens with high rating, assigned by the government, receive preferential treatment across a wide range of programs and activities.
- In the United States, U.S. Customs and Border Protection has used secret analytic tools to assign "risk assessments" to U.S. travelers.²⁸ These risk assessments, assigned by the U.S. Government to U.S. citizens, raise fundamental questions about government accountability, due process, and fairness. They may also be taking us closer to the Chinese system of social control through AI.

EPIC believes that "Algorithmic Transparency" must be a fundamental principle for all AI-related work.²⁹ The phrase has both literal and figurative dimensions. In the literal sense, it is often necessary to determine the precise factors that contribute to a decision. If, for example, a government agency considers a factor such as race, gender, or religion to produce an adverse decision, then the decision-making process should be subject to scrutiny and the relevant factors identified.

Some have argued that algorithmic transparency is simply impossible, given the complexity and fluidity of modern processes. But if that is true, there must be some way to recapture the purpose of transparency without simply relying on testing inputs and outputs. We have seen recently that it is almost trivial to design programs that evade testing.³⁰

In the formulation of European data protection law, which follows from the U.S. Privacy Act of 1974, individuals have a right to access "the logic of the processing" concerning their personal information.³¹ That principle is reflected in the transparency of the FICO score, which for many years remained a black box for consumers, making determinations about credit worthiness without any information provided to the customers about how to improve the score.³²

Building on this core belief in algorithmic transparency, EPIC has urged public attention to four related principles to establish accountability for AI systems:

- "Stop Discrimination by Computer"
- "End Secret Profiling"
- "Open the Code"
- "Bayesian Determinations are not Justice"

The phrases are slogans, but they are also intended to provoke a policy debate and could provide the starting point for public policy for AI. And we would encourage you to consider how these themes could help frame future work by the Committee.

The continued deployment of AI-based systems raises profound issues for democratic countries. As Professor Frank Pasquale has said:

Black box services are often wondrous to behold, but our black box society has become dangerously unstable, unfair, and unproductive. Neither New York quants nor California engineers can deliver a sound economy or a secure soci-

²⁵ Model Penal Code: Sentencing §6B.09 (Am. Law. Inst., Tentative Draft No. 2, 2011).

²⁶ See Julia Angwin *et al.*, *Machine Bias*, ProPublica (May 23, 2016), <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

²⁷ Josh Chin & Gillian Wong, *China's New Tool for Social Control: A Credit Rating for Everything*, Wall Street J., Nov. 28, 2016, <http://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590>

²⁸ *EPIC v. CBP* (Analytical Framework for Intelligence), EPIC, <https://epic.org/foia/dhs/cbp/afi/>.

²⁹ At UNESCO, Rotenberg Argues for Algorithmic Transparency, EPIC (Dec. 8, 2015), <https://epic.org/2015/12/at-unesco-epics-rotenberg-argu.html>.

³⁰ See Jack Ewing, *In '06 Slide Show, a Lesson in How VW Could Cheat*, N.Y. Times, Apr. 27, 2016, at A1.

³¹ Directive 95/46/EC—The Data Protection Directive, art 15 (1), 1995, <http://www.data.protection.ie/docs/EU-Directive-95-46-EC-Chapter-2/93.htm>.

³² See Hadley Malcom, *Banks Compete on Free Credit Score Offers*, USA Today, Jan. 25, 2015, <http://www.usatoday.com/story/money/2015/01/25/banks-free-credit-scores/22011803/>.

ety. Those are the tasks of a citizenry, which can perform its job only as well as it understands the stakes.³³

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Committee on these and other issues impacting the privacy and security of American consumers.

Sincerely,

MARC ROTENBERG,
EPIC President.
CAITRIONA FITZGERALD,
EPIC Policy Director.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO
CALEB BARLOW

Question 1. Quantum computing has the potential to solve problems current computers today cannot solve. How can industry work with academia and the public sector to ensure we see the benefits of such computing, while managing the potential encryption security implications?

Answer. The United States industry, academia and the public sector (DARPA/IARPA, and the DoE) must focus on accelerating the research and development of moderate-sized quantum computers and algorithms needed to solve problems such as chemical simulation for materials development and a wide range of optimization problems from improving supply chain logistics to financial portfolio decisions. There is potential for significant economic benefit by solving these types of problems that classical computers cannot practically solve.

Industry, academia and public sector (*i.e.*, NSF) must:

- Educate not only the current technical population but also emerging high school, college and graduate school students on quantum information theory and quantum computing fundamentals
- Ensure access to quantum computing systems to drive education, to drive algorithm development and to build a vibrant U.S. ecosystem of hardware, software and solution vendors

Quantum decryption leveraging Shor's Algorithm¹ will require larger fault-tolerant quantum systems. Industry and academia should be continuing to work with public sector agencies, such as NIST, to identify new encryption techniques that are not tractable for the eventual fault-tolerant quantum systems of the future, even if those systems are several decades away from being practical.

Question 2. I was pleased to hear that the emerging technologies discussed at the hearing have the potential to create new jobs and build a well-trained cybersecurity workforce. In my home state of South Dakota, Dakota State University is helping to meet this demand by doubling enrollment in its cybersecurity program in the last five years, serving as a major participant in the National Science Foundation's CyberCorps program, and hosting GenCyber camps for high school girls.

a. What steps should American educational institutions take to encourage more students to choose cyber careers?

b. How can we promote the development of entry-level cybersecurity education using emerging technology tools? How can we also promote education in higher skill levels in this field?

Answer. As discussed during the hearing and in my written testimony, there is a significant workforce shortage to fill cybersecurity positions. Information technology and security roles require specialized skills and knowledge. IBM is championing a new educational model² coupled with "new collar" approach to security hiring by going beyond traditional methods of talent recruitment and focus more on skills than actual degrees earned.

At IBM, as many as one-third of employees do not have a four-year degree. As of 2015, new collar cybersecurity professionals have accounted for around 20 percent of IBM Security's hiring in the U.S. Much of this is due to partnerships with schools for training and education as well as expanding our traditional recruiting as dem-

³³ Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* 218 (Harvard University Press 2015).

¹ Shor's algorithm—is a quantum algorithm (an algorithm that runs on a quantum computer) for integer factorization formulated in 1994.

² <https://www.ibm.com/blogs/policy/ibm-ceo-ginni-romettys-letter-u-s-president-elect/>

onstrated by IBM's Veterans Employment Accelerator, cyber training and certifying programs for military veterans.

While we do need to start educating students early about careers in cybersecurity, it needs to be recognized that the security industry needs people of all backgrounds, with creative problem solving skills, and ability to drive collaboration. Skills alignment needs to be the education reform issue. We need to match career and technical training with new collar career paths.

There are things that Congress can do to help with this alignment around skills:

- 1) Update and expand career-focused education to help more people learn in-demand skills at every stage. For example, reorient vocational training programs around skills needed in the labor market or update the Federal Work-Study Program with career-focused internships at companies
- 2) Create and fund a 21st century apprenticeship program to recruit and train/retrain workers to fill critical skills gaps
- 3) Support standards and certifications for new collar skills, just as it has been done for other technical skills, like automotive technicians and welders, providing recognition of sufficiently qualified candidates

Lastly, I've attached 3 links to new collar stories that illustrate this new collar approach to hiring—from turning a liberal arts degree into web-developer to harnessing specific on the job skills into creating malware defense technologies and lastly, an early success story from IBM's PTECH education model.

<https://www.ibm.com/blogs/policy/writing-new-collar-story-code/>

<https://www.ibm.com/blogs/policy/griff-griffin/>

<https://www.ibm.com/blogs/policy/hacking-way-new-collar-education/>

Question 3. Both technologies and threats are continually evolving. This Committee has passed significant, bipartisan legislation to advance voluntary, public-private collaboration on cybersecurity, as well as research and workforce development. For example, the Cybersecurity Enhancement Act of 2014 authorized the process for the NIST Framework for Improving Critical Infrastructure Cybersecurity. The NIST framework employs a flexible, risk-management approach that the private sector and security experts have praised. Do you believe that cybersecurity policy, especially in the context of the emerging fields we discussed at the hearing, should maintain a flexible, voluntary approach, and avoid mandatory compliance measures?

Answer. IBM commends the Committee for their continued support of a non-regulatory, risk management approach to cybersecurity. We continue to support the NIST Cybersecurity Framework and believe that a risk based approach is the best way to manage the dynamic environment that is cyberspace. Cybersecurity is, and will continue to be, a fast-paced and constantly evolving landscape. Any cyber policy that is rigid and static will fail because it will not be able to keep up with rapid changes in threats and technology. The same can be said for emerging technologies as we are on the cusp of a new era with understanding how artificial intelligence and cognitive can transform every facet of life and work. Placing compliance measures on emerging technologies, whether for security or privacy reasons, will stifle the growth of the digital future and the benefits that will come along.

Question 4. The cybersecurity of the Internet of things must be a top priority. Many of the devices in the Dyn attack last year were manufactured and located outside the U.S. How can we address cybersecurity risks from an international perspective? Given these devices provide a significant benefit to our economy, how do we also ensure American innovators are not at a competitive disadvantage in the global marketplace?

Answer. As I mentioned in my testimony, what made the Dyn attack unique was the use of common household items or devices, all with factory supplied passwords that consumers typically do not change. A sizable number of IoT devices come pre-loaded with identical credentials across multiple devices. Although these default credentials should be changed by users before the devices are made operational, they're often left as is.

Default secrets aren't secret. Attackers can use them to take over such devices for unintended purposes, making them vulnerable to sabotage or disruption. By delivering devices that prompt for a mandated password change upon first use, however, manufacturers can help ensure that default credentials can't persist.

At IBM, we have determined there are "Five Indisputable Facts about IoT Security" when building and deploying IoT devices—one of which is mentioned above re-

garding default passwords.³ We have developed a podcast series around each fact to help end users and manufacturers understand how to increase security and protect data in IoT. I've provided the link to the series here—<https://securityintelligence.com/media/podcast-iot-security-fact-1-devices-will-operate-in-hostile-environments/>—and I encourage the Committee to listen and follow up with any questions.

We must treat and consider connected equipment as computers that can be attacked, compromised and co-opted and therefore protect them with techniques used on any other computer (*i.e.*, defense in depth, network protections, supply chain protections, etc.). Monitoring and response will also be necessary (prevent, detect, respond, recover) since we all have to keep playing defense as we operate on the Internet.

In addition to the “Five Facts”, it is prudent upon industry to ensure that such common devices are not easily co-opted into botnets by utilizing secure engineering practices (*i.e.*, IBM Secure Engineering Framework, ISO 7001, etc.) in development. Furthermore, by adhering to secure lifecycle approaches, based on best practices like ISO 0243,⁴ and promote the adoption of IoT management platforms to ensure devices are maintained in a secure state, the U.S. will continue to lead in IoT innovation. IoT platforms, like Watson IoT Platform, are the control points for overall IoT operations—“configure and manage a secure environment appropriate for device, application and user requirements.”⁵

These IoT platforms should be built to handle multiple data streams from disparate sources and implement privacy by design and security by design.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. TODD YOUNG TO
CALEB BARLOW

Question. Mr. Barlow, in the areas of artificial intelligence and quantum computing, where does the United States stand compared to other countries? What should the U.S. do to regain/maintain its technological lead in these areas? What, if any, statutory or regulatory changes are required?

The United States has made significant advances in quantum computing, however, with significant strategic state investments by countries such as China in their own ecosystems we are concerned that it will be difficult for private companies to compete on equal footing. Across the world, including our neighbor to the north, Canada, there are several university and research lab based consortia being built, and the United States must continue to build and focus our own investments to support communities around quantum information science and quantum computing. This includes access to systems and research calls in promising applications of the technology. Some leading U.S. participants include but are not limited to IBM, Google, Microsoft and representatives from academia including MIT, Yale and UC Santa Barbara.

Regardless of the focus there is still a need for more investment in this critical technology to ensure continued U.S. leadership.

Below are examples of international quantum efforts:

- Canada: strong presence in quantum computing industry and academia. The University of Waterloo is one the first academic institutions to offer degrees in quantum information science. Canada's D-Wave is the largest current manufacturer of quantum computing systems (and its benefits can be explained by Canadian Prime Minister Trudeau
<https://www.youtube.com/watch?v=4ZBLSjF56S8>)
- European Union: announced last year a 1B Euro flagship initiative on quantum technologies. Australia: announced a 70M joint government. Industry and academic investment in quantum computing technology
- The Chinese Academy of Sciences announced a “hack proof” quantum satellite in January 2017. Alibaba announced in 2015 that it was building a quantum computing laboratory with support from the Chinese Academy of Science.

The United States currently has a strong position in artificial intelligence and leads in creation of new technologies, but (a) China is moving quickly on AI tech-

³ https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEF03018USEN&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US&cm_mc_uid=67767554257814879487367&cm_mc_sid_50200000=1492781598&cm_mc_sid_52640000=1492781598

⁴ <https://www.iso.org/standard/67394.html>

⁵ <https://www.ibm.com/internet-of-things/platform/iot-security> | <https://www.ibm.com/blogs/internet-of-things/security> | <https://www.ibm.com/blogs/internet-of-things/security-cognitive-iot/>

nology, driven by significant government investment and by mass deployment of applications for consumers; and (b) Canada has key academic leaders in AI. To ensure AI competitiveness, the U.S. Government needs to act now and help foster: (a) open data sets and challenge problems to drive AI research in the U.S.; (b) AI research and development in academia and corporations; and (c) invest in talent development at U.S. universities as we have too few AI and data scientist graduates entering the workforce.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. EDWARD MARKEY TO
CALEB BARLOW

Question. The Federal Government relies on Internet of Things devices and could bear a heavy burden if these devices are breached by a cyberattack. To align security incentives and promote cybersecurity, should contractors and vendors selling Internet of Things devices to the Government be required to bear their financial responsibility in the event of a material breach through mechanisms like cyber insurance?

Answer. Thank you Senator Markey for the question. I think it is important to put in context that cybersecurity concerns apply to IoT much as they do to other digital environments. Connected devices can be used as personal devices as well as part of critical infrastructure.

As with most discussions with public and private sector clients regarding general allocation of risk—whether it is in the context of IoT, data security, etc.—the balance of providing appropriate level of protection for those who might suffer injury or loss and ensuring that liability rests on the most appropriate party must be struck. Liability risks discussed with respect to IoT are *not* new or specific to IoT. We believe that the well-established existing legal framework is fit to address liability issues in the field of IoT. Contractual liability offers the most flexible way to adapt to the specificities of each product and situation and existing tort law imposes liability for damages caused by products with design defects or manufacturing defects.

Requiring cyber insurance for the producer could result in an increase cost of production which the producer would have to shift on the price of the products. This would result in an increase cost of the products which may in fact represent an obstacle for distribution in the market and presenting the spread and development of technology.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TAMMY DUCKWORTH TO
CALEB BARLOW

Question 1. To all of the Witnesses, beyond standards and frameworks, from an industry perspective, what are the top three to five best practices you've identified to protect critical infrastructure that enables companies and governments to enact proactive measures instead of just focusing on the response to threats or disasters? Specifically, I want to know how we move from reaction to proaction.

Answer. At IBM, we are continually evolving our capabilities to stop threats at speed and scale. However, we are finding that many organizations are drowning in a sea of unmanageable, disconnected point products and services, each designed with a specific task making it that much more challenging to stay at pace with the ongoing threat. Some organizations report they are using as many as 85 security products—from more than 40 vendors—at once. As each tool is added, the cost associated with installing, configuring, managing, upgrading and patching continue to grow. And with the skills gap plaguing the industry, where the necessary expertise isn't always available, it's easy to see how more threats are continuing to generate more vendors, more tools—and more headaches. Yesterday's security era of moats and firewalls is antiquated. The reality is that even with the best perimeter defenses, some attacks will get through. From a technical standpoint, we must move towards managing and remediating threats like an *immune system*.

The analogy is this: As humans, we have finely tuned and highly adaptive immune systems to help us fight off all kinds of attacks that would otherwise destroy us. Our bodies are intelligent, organized, efficient systems that can instantly recognize an invader and take action to block its entry or destroy it. Therefore, we need to manage security like an immune system and develop an integrated and intelligent security system with analytics and cognitive technologies at its core.

As I mentioned in my testimony, the health analogy also extends to the need for the public and private sector to more actively share threat data—similar to how the Center for Disease Control and World Health Organization rapidly share data and

collaborate to battle pandemics and other health outbreaks. IBM is constantly evolving this approach with focused investments in cognitive, collaboration and cloud that drive our innovation.

Lastly, but just as important, it is imperative that organizations prepare and train for security incident response—from a lost employee laptop to a highly sophisticated breach—for a prompt and highly coordinated response in the event of an issue. Organizations need to deploy incident response technologies to automate and speed processes, from a multitude of regulatory filings, to client and employee notification.

Question 2. As this committee moves forward in the 115th Congress, we are considering oversight and legislation within the committee's jurisdiction of science, technology, transportation and the critical infrastructure that supports them. For all the witnesses in closing, what should this committee keep in mind in order to help make sure we're developing the framework for infrastructure that is proactive, resilient and lasting as cyber threats continue to evolve?

Answer. IBM continues to support the risk management approach and stakeholder engagement process that produced the NIST Cybersecurity Framework that is voluntary, flexible and applicable for every sector of the economy. We ask that the Committee continue to use the Framework as a cornerstone for any oversight of different critical infrastructure sectors and their approach to cybersecurity risk management. The Framework is a living guidance document and we expect further improvements, changes, additions as industry continues to innovate and address new challenges in cyberspace.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO
VENKY GANESAN

Question 1. I was pleased to hear that the emerging technologies discussed at the hearing have the potential to create new jobs and build a well-trained cybersecurity workforce. In my home state of South Dakota, Dakota State University is helping to meet this demand by doubling enrollment in its cybersecurity program in the last five years, serving as a major participant in the National Science Foundation's CyberCorps program, and hosting GenCyber camps for high school girls.

a. What steps should American educational institutions take to encourage more students to choose cyber careers?

b. How can we promote the development of entry-level cybersecurity education using emerging technology tools? How can we also promote education in higher skill levels in this field?

Answer. Community colleges can be an invaluable asset in both increasing cybersecurity literacy and competence in our country. The Federal Government should consider market incentives for community colleges to both develop cybersecurity curriculum and launch courses in the subject. Many of the skills required to be an entry-level operator or analyst in the cybersecurity space can be acquired over a 12–18 month period and are perfect as an associate or junior college degree. In addition, I recommend the creation of an elite U.S. cyber academy similar to West Point and the U.S. Naval academy where very high performing high schoolers in math and computer science can be recruited and trained specially for cyberwarfare. Similar to the programs in Israel, this can be a very effective way to build a pool of extremely well qualified and trained cyber talent.

Question 2. Both technologies and threats are continually evolving. This Committee has passed significant, bipartisan legislation to advance voluntary, public-private collaboration on cybersecurity, as well as research and workforce development. For example, the Cybersecurity Enhancement Act of 2014 authorized the process for the NIST Framework for Improving Critical Infrastructure Cybersecurity. The NIST framework employs a flexible, risk-management approach that the private sector and security experts have praised. Do you believe that cybersecurity policy, especially in the context of the emerging fields we discussed at the hearing, should maintain a flexible, voluntary approach, and avoid mandatory compliance measures?

Answer. Yes, I absolutely believe that cybersecurity policy in the context of the emerging fields should maintain a flexible, voluntary approach and avoid mandatory compliance measures. This field is too dynamic and our adversaries are too fleet-footed for static mandatory compliance measures to be effective. Market based approaches driven by cyberinsurance could be another way to create compliance incentives for companies.

Question 3. The cybersecurity of the Internet of things must be a top priority. Many of the devices in the Dyn attack last year were manufactured and located out-

side the U.S. How can we address cybersecurity risks from an international perspective? Given these devices provide a significant benefit to our economy, how do we also ensure American innovators are not at a competitive disadvantage in the global marketplace?

Answer. We need to create an awareness program around the security risks posed by IoT devices and create market incentives for all vendors (both domestic and international) to do the following:

- Participate in the best practices and standards proposed by the NIST cybersecurity framework;
- Provide cyber warranties for their products which require them to both support and update their products with the most recent security patches; and
- Have a minimum amount of cyberinsurance coverage so that there is some financial compensation in case of a material breach.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JERRY MORAN TO
VENKY GANESAN

Question. According to the GAO's *High Risk Series* report, the Federal Government annually spends over \$80 billion on information technology (IT), but over 75 percent of this spending is for "legacy IT". In fact, since FY 2010, agencies have increased spending on "legacy IT;" thereby, crowding out spending on development, modernization, and enhancement activities. Last Congress, I led legislation called the Modernizing Outdated and Vulnerable Equipment and Information Technology (MOVE IT) Act with my colleague Senator Udall to reduce wasteful Federal Government spending on outdated "legacy IT" systems and enhance information security.

In your testimony, you provided five recommendations to this committee to improve comprehensive cybersecurity practices of the U.S. Federal Government and industry as a whole. The first recommendation on that list included, "Modernizing government procurement systems so that the government has access to the best technologies."

a. Could you please go into further detail on how the Federal Government's procurement policies and resources could be improved and better facilitate the adoption of necessary innovations such as cloud computing?

b. How can modernizing Federal Government IT make us more secure?

c. There have also been considerations to streamline the certification process of the Federal Risk and Authorization Management Program, also known as FedRAMP, so that smaller companies without large legal departments might be able to get certified to do business with the Federal Government. Do we need to make it easier to allow smaller companies help the government?

Answer. The Federal Government's procurement processes today for cybersecurity products is very cumbersome, restrictive, and bureaucratic. Most small or innovative cybersecurity companies will not even consider selling to the Federal Government, which is a tragedy since most of the innovation is happening there. The primary reasons are various compliance requirements such as FIPS and FedRamp, both of which are expensive and time consuming. Companies estimate it takes millions to get FIPS certification and over 2 years to be FedRamp certified. There have been some fast track programs through the DOD, DHS, and In-Q-Tel, but these do not apply to most Federal agencies. Similar to the JOBS Act, which provided exemptions from some certain regulations for companies below a certain size, I would recommend a modified procurement process for companies below \$1 billion in revenue which would enable smaller, nimble, venture-backed startups to sell to the Federal Government.

Modernizing Federal Government IT is one of the most important things we can do. It will not only make our government secure and protect invaluable data but it will also bring down our costs in the long run. Today the government is captive to old on-premise systems, which are both functionally weak and very expensive to maintain. By shifting to cloud based systems, the government can both get much better functionality and user interface and significantly save on operational costs. The move to the cloud would also make our systems more secure since private cloud vendors are investing a lot more in cybersecurity than on-premise vendors.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. EDWARD MARKEY TO
VENKY GANESAN

Question. The Federal Government relies on Internet of Things devices and could bear a heavy burden if these devices are breached by a cyberattack. To align security incentives and promote cybersecurity, should contractors and vendors selling Internet of Things devices to the Government be required to bear their financial responsibility in the event of a material breach through mechanisms like cyber insurance?

Answer. As part of the procurement process, the Federal Government should require contractors and vendors who sell Internet of Things devices to do the following:

- Participate in the best practices and standards proposed by the NIST cybersecurity framework;
- Provide cyber warranties for their products which require them to both support and update their products with the most recent security patches; and
- Have a minimum amount of cyberinsurance coverage so that there is some financial compensation in case of a material breach.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TAMMY DUCKWORTH TO
VENKY GANESAN

Question 1. To all of the Witnesses, beyond standards and frameworks, from an industry perspective, what are the top three to five best practices you've identified to protect critical infrastructure that enables companies and governments to enact proactive measures instead of just focusing on the response to threats or disasters? Specifically, I want to know how we move from reaction to proaction.

Answer. Protecting critical infrastructure is indeed one of the most important things we can do to defend our Nation and economy and preserve the quality of life we all seek.

Here are my recommendations on how we can be proactive on this issue:

1. Clearly define and catalog all the elements of our critical infrastructure
2. Establish minimum security standards and best practice frameworks for these elements of critical infrastructure
3. Define and catalog the processes by which both employees and 3rd party vendors can access this critical infrastructure
4. Require that all vendors of critical infrastructure must participate in the NIST cybersecurity framework and have adequate cyberinsurance coverage in case of a material breach
5. Update and revise items 1–3 on a yearly basis so that we account for new bugs or hacking techniques

Question 2. As this committee moves forward in the 115th Congress, we are considering oversight and legislation within the committee's jurisdiction of science, technology, transportation and the critical infrastructure that supports them. For all the witnesses in closing, what should this committee keep in mind in order to help make sure we're developing the framework for infrastructure that is proactive, resilient and lasting as cyber threats continue to evolve?

Answer. Cybersecurity is an extremely fast moving field where the adversary is working feverishly every day to find weaknesses. It is an asymmetric problem as the adversary only needs to find one weakness to overcome all the protections we have in place. This means that the government has to take a market based dynamic approach to fix the problem. It is important to create market incentives for critical infrastructure vendors to invest in cybersecurity by both specifying best practice frameworks and mandating cyberinsurance coverage. Cyberinsurance can be a good market based approach to provide dynamic feedback and incentive for vendors to proactively improve their cybersecurity approach.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO
STEVE GROBMAN

Question 1. Quantum computing has the potential to solve problems current computers today cannot solve. How can industry work with academia and the public sector to ensure we see the benefits of such computing, while managing the potential encryption security implications?

Answer. There is a long and successful tradition of the Federal Government funding science and technology research at our Nation's universities. Federal funding of research and development managed by such agencies as the National Science Foundation has, over the years, helped produce a wide range of innovations in hardware, software and biotechnology that have enabled American companies to stay at the forefront of the information technology revolution. When I think of cutting-edge examples of universities that partner well with industry, Stanford University, the University of California, and North Carolina State University come to mind. All these great schools have helped spawn countless companies—Sun Microsystems, Google, and Red Hat are just a few examples—that have supported the growth of our innovation economy. Policymakers should continue to invest in university-based research to promote advances in such cutting-edge technologies such as quantum computing to help ensure that the United States remains in the top rank of computing. Investing in university-based research at institutions that have strong partnerships with industry have proven to work well in the past and can continue to pay huge dividends in the future.

Additionally, we need to ensure there is proper funding for both research institutions and NIST to address the need for more quantum-safe encryption algorithms. Today, the AES algorithm, which is used for bulk data encryption, is considered quantum-safe. An example of a quantum un-safe algorithm is the public key algorithm RSA. Unfortunately, most encryption uses these algorithms in combination, and being able to break either one places data at risk. Research efforts are needed to ensure we can replace the quantum un-safe algorithms that are extensively used today to secure our infrastructure.

Question 2. I was pleased to hear that the emerging technologies discussed at the hearing have the potential to create new jobs and build a well-trained cybersecurity workforce. In my home state of South Dakota, Dakota State University is helping to meet this demand by doubling enrollment in its cybersecurity program in the last five years, serving as a major participant in the National Science Foundation's CyberCorps program, and hosting Gen Cyber camps for high school girls.

A. What steps should American educational institutions take to encourage more students to choose cyber careers?

Answer. Addressing our Nation's cyber skills shortage requires us to think and act in a holistic manner. We need to invest more in science, technology, engineering and math (STEM) education for grade school and middle school students. As James Brown, executive director of the STEM Education Coalition in Washington, DC, said recently, "The future of the economy is in STEM," adding that the Bureau of Labor Statistics projects that employment in STEM jobs will grow to more than nine million between 2012 and 2022. That is probably a conservative estimate. While various initiatives have sprung up to address the STEM education problem, we're not there yet—and we need to be. We need a broad-based STEM investment plan to solve this long-term problem. We should ensure that all middle and high school students have the opportunity to take substantial cybersecurity courses at school. For high school students, we need to expand our idea of what it means to take shop classes in school that can prepare students for careers repairing cars. The shop classes of the future need to also focus on building IT and cyber skills so students can develop these critical, job ready skills before they graduate.

But it's not just STEM awareness that children need at an early age. It's also awareness of security and privacy. As adults we hear about breaches in the news, and some of us understand cyber is a corporate board room topic, but does the average grade school and middle school student learn about the importance of cyber safety? Do they understand what that means beyond "don't share your password"? Where does security sit on the average college student's list of priorities? We have a great opportunity to increase awareness about security as it affects the workforce at large, with 1.5 million unfilled jobs today and growing, providing the opportunity for steady, high-paying jobs. We also have an opportunity to increase awareness in a way that appeals to the millennial generation—a group passionate about causes, especially human interest ones—and generation X youth, who are learning about how to keep themselves and their friends safe. We need both traditional and creative approaches to reach these students, possibly through gamification.

The Federal Government needs to partner with states to support an expansion of cybersecurity training programs at our Nation's community colleges. The National Science Foundation-managed Scholarship for Service (SFS) CyberCorps program is an example of a successful Federal program. While the CyberCorps program serves college juniors and seniors who are already far along the learning path, another program, or an expansion of the SFS program, could attract high school graduates who don't yet have specific career aspirations. Private companies could partner with a community college in their area to establish a course of study focusing on cybersecurity. The Federal Government could fund all or part of the tuition remission for students. Interested students would be taught both by college faculty and private sector practitioners. For example, an IT company could offer several faculty members/guest lecturers who would participate during a semester. Students would receive free tuition—paid for by a Federal program, perhaps with private sector contributions—and, if they can show a financial need, a stipend for living arrangements, which four-year college students can get through the CyberCorps program. Students would receive a two-year certificate in cybersecurity that would be transferrable to a four-year school. Like the CyberCorps program, graduates would spend the same amount of time as their scholarship period working in a guaranteed government job.

At McAfee, we have been strong supporters of the CyberCorps scholarship program, given the need to train many more college graduates at the four-year university level. With additional funding, the CyberCorps SFS program certainly could be expanded to more institutions and more students within each of those schools. To date, the Federal Government has made a solid commitment to supporting the SFS program, having spent \$45 million in 2015, \$50 million in 2016, and the most recent Administration's budget requested \$70 million. As a baseline, an investment of \$40 million pays for roughly 1,500+ students to complete the scholarship program. Given the size and scale of the cyber skills deficit, policymakers should significantly increase the size of the program, possibly something in the range of \$180 million. At this level of funding, the program could support roughly 6,400 scholarships. Such a level of investment would make a dent in the Federal cyber skills deficit, estimated to be in the range of 10,000 per year. At the same time, this level of investment could help create a new generation of Federal cyber professionals that can serve as positive role models for a countless number of middle and high school students across the country to consider the benefits of a cyber career and Federal service. Indeed, this positive feedback loop of the SFS program might well be its biggest long-term contribution.

B. How can we promote the development of entry-level cybersecurity education using emerging technology tools? How can we also promote education in higher skill levels in this field?

Answer. Fortunately, not all cyber jobs or successful cyber-related careers need a four-year degree in computer science. Policymakers should look at supporting and promoting the expansion of two-year cybersecurity programs, as many jobs can be staffed by individuals with community college degrees. Another way to promote cybersecurity education is by investing in cross-training programs that offer certifications from non-traditional educational organizations. With the proper background in STEM, even on-the-job training can be beneficial.

We are starting to see newer, more innovative technologies being made available to students in K–12 settings. However, far too often these educational technologies fail to properly focus on cybersecurity training. Policymakers should prioritize IT investments in schools that also include cybersecurity capabilities to enable a more balanced training regime. Cybersecurity companies should replicate learnings from other sectors of the IT ecosystem and provide affordable cybersecurity solutions to students as learning tools, given the important role of hands-on learning. Policymakers should consider a range of incentives—possibly tax credits or procurement preferences—to encourage manufacturers and security vendors to make their software and solutions available to schools for the purpose of supporting student engagement and learning.

Question 3. Both technologies and threats are continually evolving. This Committee has passed significant, bipartisan legislation to advance voluntary, public-private collaboration on cybersecurity, as well as research and workforce development. For example, the Cybersecurity Enhancement Act of 2014 authorized the process for the NIST Framework for Improving Critical Infrastructure Cybersecurity. The NIST framework employs a flexible, risk-management approach that the private sector and security experts have praised. Do you believe that cybersecurity policy, especially in the context of the emerging fields we discussed at the hearing, should maintain a flexible, voluntary approach, and avoid mandatory compliance measures?

Answer. Yes. As stated in my testimony, I believe the cybersecurity threat landscape changes extremely quickly. What is deemed the most serious threat today may not be the most important tomorrow. If regulations directed manufacturers to guard against today's threats, tomorrow's might very well slip through the cracks. Additionally, compliance is not security. It simply proves the manufacturer is able to check a box saying that they are in compliance. Regulations in the security field have resulted in corporations diverting real monies away from true security. Regulating an area like cybersecurity is very tricky and unintended consequences could easily outweigh any benefits.

Policymakers should maintain a flexible, voluntary approach to cybersecurity and avoid the temptation to impose mandatory compliance on organizations. The NIST approach to cybersecurity is spot on—it's a voluntary, flexible, risk-based approach that is done in true partnership with the private sector. This model has shown to be quite effective because both the government and industry participants have 'bought in' to the issue and work in concert with each other to achieve a positive end result. The NIST Cybersecurity Framework truly is having a positive impact on how organizations view their cyber risk management processes. Partnerships such as this are productive and will pay dividends as policymakers and the private sector work together to secure the next generation of technology innovations.

Question 4. The cybersecurity of the Internet of things must be a top priority. Many of the devices in the Dyn attack last year were manufactured and located outside the U.S. How can we address cybersecurity risks from an international perspective? Given these devices provide a significant benefit to our economy, how do we also ensure American innovators are not at a competitive disadvantage in the global marketplace?

Answer. The cat's out of the bag. The Internet provides global connectivity of devices, including traditional devices and IoT devices. We can't always use the same logic that works in the physical world and apply it to the digital world. We can't think of devices being contained in one country or another and not having an impact on other countries, especially in the U.S., which is committed to a free and open communications architecture. The most important thing is to recognize this type of attack is possible. We need to prepare organizations to be able to defend against these types of attacks, while educating IoT device manufacturers on a global basis that it is critical for them to take security seriously by building strong security and privacy architectures and update mechanisms into their devices.

Policymakers should champion the principle of security and privacy by design to help incent broad adoption and trust in IoT products and infrastructure. Proper protection of individual security and privacy in products does not just happen. It needs to be designed and engineered from the beginning of the product development process. Adding or 'bolting on' security features to a system, network or device after it's already up and running has proven to be ineffective. IoT is a great example of where security and privacy protections need to be built in from the start. This approach is not only more effective; it is less cumbersome and less expensive than trying to lock down systems that are leaking personal information or are inherently insecure.

In order to ensure the U.S. continues to be an innovator in all types of connected devices, we must recognize the development process needs to be at the same level of friction as it is in any other part of the world. We need to be cautious given the reality that over-regulating in the U.S. will simply cause device design and manufacturing companies to move to other regions of the world. We need to ask ourselves if we wish to impose other costs on our economy by forcing U.S. citizens to pay higher taxes on imported devices. There really are no borders; we live in a borderless virtual world. As part of a larger strategy to drive security and privacy into the early design phase of IoT devices, policymakers should support industry led, global security and privacy standards. Global standards are much more effective than country-specific security and privacy regulations in producing the outcome we all want—more secure and more privacy-friendly IoT devices.

We need to accelerate leadership in IoT security and privacy. How can policymakers accelerate IoT deployments to ensure U.S. leadership? Candidly, the U.S. is behind. Other countries such as China, Brazil and the UAE are aggressively investing in and deploying IoT to transform their economies, address societal problems, and spur innovation. Many have adopted national IoT plans with time-bound goals and are investing heavily in IoT R&D and infrastructure. The U.S. needs to do the same and needs to act now. Congress can advance our Nation's IoT momentum by collaborating with industry to establish a national IoT strategy that includes a strong security and privacy foundation and by encouraging public-private partnerships that uniquely focus on security, while aiming to improve manufacturing productivity, optimize transportation efficiency, reduce energy consumption, sustain our

environment and accelerate smart cities and towns. Promoting industry alignment around these large-scale IoT deployments based on secure, open and interoperable solutions will deliver immeasurable benefits and showcase U.S. leadership.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. EDWARD MARKEY TO
STEVE GROBMAN

Question. The Federal Government relies on Internet of Things devices and could bear a heavy burden if these devices are breached by a cyberattack. To align security incentives and promote cybersecurity, should contractors and vendors selling Internet of Things devices to the Government be required to bear their financial responsibility in the event of a material breach through mechanisms like cyber insurance?

Answer. No. While “organizational cyber-risk” insurance is needed and its markets and offerings are growing, it is not the silver bullet. First, not all cybersecurity challenges derive from vendor design mistakes. Products often provide capabilities that can and should be configured by the organization’s staff or end user. Improper customer configuration can cause vulnerabilities and exposure data.

In today’s IT ecosystem, there are complex supply chains and design chains that have become baked into the way that virtually all manufacturers operate. Thus, it is not practicable for the final assembler of a device to validate the technology in all the subcomponents. Consider the Takata airbag recall. This component manufacturer supplies its airbags to 19 different automakers. In this case, it was not the product vendor or the car company but the supplier that was at fault, and is now working to correct the situation.

Second, this would have unintended consequences on innovation. If we are trying to foster the development of new and innovative solutions by American companies to sell in a global marketplace, we need to understand the effect this may have on the startups that have real, valuable ideas for unique products and services. If they have to raise the additional funds from investors to pay the cover charge to get in the door, their potentially valuable ideas will languish. It could even have an effect on the investment community’s approach to funding IoT innovators. Even established product vendors could use defensive tactics and be very selective as to what new types of products they offer. Meanwhile, organizations developing IoT products in other nations would not have this restriction. Would products built and developed in other countries have the same requirements when they’re sold into the U.S. market? If so, they will likely have grown their product sales, external to the U.S., to a point where they are able to pay-to-play in the U.S. World-class solutions may not be available in the U.S. until they have shown their success in foreign markets. This approach would put U.S. innovators at a critical disadvantage both here and on the global stage. Unintended consequences could extend beyond the life of a company if it went out of business. For example, there will always be a problem with orphaned devices when manufacturers cease to exist. If too harsh a level of responsibility is imposed on manufacturers, policymakers may encourage the creation of corporate shell structures to shield corporate liability. This unfortunate result could add complexity and cost to the IoT ecosystem while undercutting the goal of improved security.

Randal Milch, Former General Counsel, Verizon; Distinguished Professor, NYU School of Law, testifying before the Commission on Enhancing National Cybersecurity on May 16, 2016, discussed three attributes of a well-functioning insurance market. The first is information, the second is the ability to have after-action forensic reports and the third is focusing on and citing standards. Today, the information foundation to establish a marketplace for this rapidly evolving diverse IoT product environment is not there. Getting after-action forensic reports from consumers to determine liability may be very problematic and the foundational standards used today within the IoT space are far from defined, let alone universally accepted.

For example, how long was OPM exposed to a major cybersecurity attack before its compromise was discovered? Was it one product that was at fault in the OPM breach or was it a system or systems circumvented to allow exfiltration of 21.5 million records. Do we really know? What if the agency had been warned of issues they needed to address?

At this point in time, the IoT product environment and the general cyber insurance market is extremely immature and, in my opinion, not capable of supporting this solution. The unintended consequences this approach may create could have a negative and long lasting impact on America’s ability to innovate and capture the growing IoT market share globally.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TAMMY DUCKWORTH TO
STEVE GROBMAN

Question 1. Mr. Grobman, in your testimony you referred to NIST's Framework for Improving Critical Infrastructure Cybersecurity as a "best-in-class" example of a successful private-public partnership between critical infrastructure companies and government agencies. In your view how can we build on foundations like these to improve the security of critical infrastructure at all levels—state, local, county and federal?

Answer. The Framework for Improving Critical Infrastructure Cybersecurity, known as the NIST Cybersecurity Framework, is widely acknowledged as a highly successful model of public-private partnership. The Office of Management and Budget is already working to push Federal agencies to adopt the Framework, the new Administration's draft executive order mandates government agencies to deploy the framework, and the private sector is rapidly adopting it.

Here's our analysis of why it has been successful:

- The need was real
- The process was open
- NIST listened first
- They were prepared
- They engaged all stakeholders
- The framework was voluntary—not regulatory

I'd like to expand on each of these aspects, not simply to compliment NIST but to offer the process as a model for future public-private partnerships.

The need was real: PPPs created around a topic or issue that is real to both the public and the private sectors have a much better chance of getting the exposure and participation needed to achieve the goal of the partnership. In the case of the Cybersecurity Framework, it was very obvious to both groups that the need existed. While NIST had a hard time-frame to be successful in—one year—they have a long history in risk management and understood the need well. For too long, regulatory compliance had forced industry to spend valuable security dollars to prove something to the regulators instead of using those resources to help protect enterprises. The cost of compliance was impacting our ability to secure ourselves.

Openness of the process: From the very beginning, NIST made it clear this was going to be a very open process. In the initial meeting, NIST staff described what would be occurring, from the RFI-submitted comments that would be made public on NIST's website to the anticipated workshop process and general timeline for various milestones. Along the way, NIST staff were quick to ensure that industry participants understood what was happening so there would be no surprises. This created a growing sense of trust as the effort evolved and made the process more effective during the development of the Framework.

Listening: One of the more interesting and effective parts of the development was the way NIST staff listened to the workshop participants. They used a moderated dialog approach that allowed all attendees to voice their opinions on a set of topics the NIST staff wanted to learn about. There were very active discussions that were highly informative from members of various sectors and industries. Dr. Gallagher, NIST's director at the time, stated quite clearly this was not NIST's Framework; this was the community's framework. Having the public side of a public-private partnership listen instead of dictate allowed private sector participants to voice their opinions in a much more open and direct way. This, too, built trust as the effort went along.

Being prepared: Each of the workshops seemed very well organized, and the topics, panels, questions and outcomes were well thought-out before each workshop began. This gave participants reassurance their time was being well spent. Open forums with no direction or planning do not give those involved much confidence the effort will succeed. Being prepared also meant participants needed to do their homework as well. While not always the case, as the workshops advanced, they did.

Engaging all: One of the smartest things NIST did as part of the Framework development process was to understand they needed to get outside the Beltway for the effort to be successful. They held the workshops in different locations around the country so the local owners/operators of the critical infrastructure could have their voices heard. This ensured there was a diverse group at each of the workshops and all were able to participate. The processes used during the workshops encouraged all in the room to contribute and they did. A highly interactive, collaborative environment is one where real dialog can occur and produce positive results.

Voluntary—Non-regulatory nature: The fact that NIST is a non-regulatory body also helped their credibility and the private sector's attitude towards participating and contributing. This was a topic area that had a lot of people concerned initially, but as the effort progressed, more and more private sector participants relaxed and believed in the voluntary intent of the effort. NIST also made it clear in each workshop that they were requiring non-attribution from any and all regulators in the room. Each agreed to the rules, making it much more comfortable for real, open and honest dialog to occur. While others have tried to copy NIST's success, often they have left out one or more of the characteristics that made the Cybersecurity Framework effort a success. In reality, both the public and the private sector participants must buy in. To do so requires trust in the process, the effort and the vision.

Question 2. To all of the Witnesses, beyond standards and frameworks, from an industry perspective, what are the top three to five best practices you've identified to protect critical infrastructure that enables companies and governments to enact proactive measures instead of just focusing on the response to threats or disasters? Specifically, I want to know how we move from reaction to proaction.

Answer. As mentioned above, the NIST Cybersecurity Framework is a great place for any organization to start. Over the past decade, the U.S. business community has been so focused on compliance reporting that many organizations did not have the resources to invest in true security. The Framework has really changed the conversation from compliance to risk-management. Cyber is now being integrated into existing corporate risk management planning and processes.

Organizations are now improving their cyber programs by using the Framework to implement repeatable processes. The end result is the Framework is providing the foundation for helping improve the organizational security posture by focusing on people, process and technologies. While U.S. organizations used to focus on proving to a regulator they are compliant at one point in time, increasingly those same organizations are focusing on how to improve their corporate cybersecurity risk management program on a continuous basis. Today, the Cybersecurity Framework is focused on traditional computing systems. As we look to real operational technology, it will be critically important to continue and accelerate the process of evolving the framework to not only comprehend the elements of computing common to all industries, but also to look at things unique to specific critical infrastructure sectors.

Another trend McAfee is encouraging is moving internal network defenses from locally-focused to enterprise-focused. In the past, network and point products were highly siloed, meaning they did not communicate event and incident information in a way other components in the network could understand and use. For example, in the past, if a user's PC detected malware, it would quarantine or delete the offending malware and write a log record to a logfile that may or may not have been sent to an administrator's console. Often the fact that it happened went undetected due to the high quantity of event information administrators needed to deal with. The event needed to be tracked and responded to but it was not. Today when that situation occurs, the PC can create a hash of the detected malware and send it to a central repository in near real time. That information is now immediately available to other components in the network subscribed to the repository. For example, when the mail gateway receives an e-mail message with an attachment, the mail gateway is able to create a hash of the attachment and then compare that hash with those stored in the central threat intelligence repository. If a match is found, the e-mail message can be blocked at the boundary, protecting subsequent users. This type of internal threat information sharing between network components provides a much quicker response and informed protections not available in the recent past. All the while, this capability is being driven by the policy rules configured and managed by the site's network staff. We believe this trend toward automation in the right places allows corporate network defenses to act together and at much more wire-speeds than has been possible in the past. It also frees up critical network and security staff to do more valuable work.

Much has been said about cyber threat intelligence (CTI) sharing but we are still in the early days of demonstrating its value. It is understandable that if one organization sees something on their network and they share that information with a sharing partner, the partner could use that information to better protect themselves. One's detection is another's prevention. In the Cybersecurity Information Sharing Act of 2015, DHS was directed to stand up the Automated Information Sharing (AIS) program, providing the ability to share cyber threat indicators between the Federal Government and private sector at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender address of a phishing e-mail. While indicators can be useful, AIS has no capability to share enriched cyber threat intelligence. Threat intelligence is much more than a single piece of informa-

tion contained in an indicator and can contain threat information such as exploit targets, adversarial tactics, techniques and procedures, incidents, courses of action, identified threat actors, and additional valuable context. Often in the security community, one organization will discover something they consider malicious and share it with other trusted sharing partners. A sharing partner may discover other characteristics of the threat and can pass that enriched information back to the original organization. Over time, the shared data can provide all participating organizations with a much more holistic picture of the specific threat, potentially including how to mitigate or defend against it. Today, the AIS program does not provide a means to send enriched intelligence out to their participating sharing community. As we move to mature cyber threat sharing capabilities, it is critical we figure out how to share real cyber intelligence instead of simple indicators.

Question 3. As this committee moves forward in the 115th Congress, we are considering oversight and legislation within the committee's jurisdiction of science, technology, transportation and the critical infrastructure that supports them. For all the witnesses in closing, what should this committee keep in mind in order to help make sure we're developing the framework for infrastructure that is proactive, resilient and lasting as cyber threats continue to evolve?

Answer. It is important to think about the objective to minimize risk and reduce the damaging impact of cyber threats versus attempting to create a legislative process to remove or eliminate them. An example of this is NOAA and FEMA reducing the impact of natural disasters such as hurricanes. By improving our ability to track hurricanes, and improving our response capabilities, we have been able to drastically reduce the number of deaths caused by hurricanes over the last few decades. But we all recognize they will occur; there will be damage to property and occasional unavoidable loss of life. Our goal is to minimize that damage and loss instead of having the unrealistic expectation of eliminating hurricanes completely. The point here is for policymakers to focus on minimizing risk and reducing impacts as opposed to attempting to have an expectation that anyone will be able to remove cybersecurity threats from the world we live in today on a permanent basis.

It is also critical to keep in mind that this is a shared problem. No one organization, regardless of size, can solve this problem, either in the private or the public sectors. It will take all of us working together with open lines of communication and shared goals to be able to get to the point where adversarial evolution in tactics and tools has negligible effect on our daily lives. Flexibility is critical. We need to ensure that any legislation passed is enabling in nature and not restrictive in our abilities and actions. When all the stakeholders buy-in to a shared set of goals and outcomes, the prospects of long term success greatly increase.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO
MALCOLM HARKINS

Question 1. I was pleased to hear that the emerging technologies discussed at the hearing have the potential to create new jobs and build a well-trained cybersecurity workforce. In my home state of South Dakota, Dakota State University is helping to meet this demand by doubling enrollment in its cybersecurity program in the last five years, serving as a major participant in the National Science Foundation's CyberCorps program, and hosting GenCyber camps for high school girls.

a. What steps should American educational institutions take to encourage more students to choose cyber careers?

Answer. Our educational institutions need to provide students in schools across the Nation with the opportunity to learn about cyber careers. We need to have programs that will develop new skills as well as help students understand our industry challenges with the goal of helping them find their own purpose and passion. These programs need to span science, technology, engineering, math as well as humanities, sociology, and psychology. Our educational institutions need to reach across every degree program and understand the current as well as future digital dependencies for those fields. Each area of study should embrace its specific cyber learning needs, not only for security but also for data privacy. These educational programs not only need to develop our skills to deal with the risk concerns after technology is deployed, but we need to build a much stronger focus on improving the development of technology with fewer vulnerabilities through teaching security development lifecycle and privacy-by-design skills. If we take this sort of broad approach, everyone will gain the needed cyber skills for their chosen career in addition to the specific cyber careers we have a current critical need to foster.

b. How can we promote the development of entry-level cybersecurity education using emerging technology tools? How can we also promote education in higher skill levels in this field?

Answer. One way we can promote the development of entry-level cybersecurity education using emerging technology is through setting up cyber ranges at schools so that students can learn about the technology, have simulated experiences using these tools, and practice the processes they would use in a real cyber career. Additional entry level education could be done through internships as well as mentoring programs within the industry. We can promote higher education in this field by offering research grants, scholarships, as well as by encouraging industry to create endowments for educational institutions to perform research and support advanced educational efforts.

Question 2. Both technologies and threats are continually evolving. This Committee has passed significant, bipartisan legislation to advance voluntary, public-private collaboration on cybersecurity, as well as research and workforce development. For example, the Cybersecurity Enhancement Act of 2014 authorized the process for the NIST Framework for Improving Critical Infrastructure Cybersecurity. The NIST framework employs a flexible, risk-management approach that the private sector and security experts have praised. Do you believe that cybersecurity policy, especially in the context of the emerging fields we discussed at the hearing, should maintain a flexible, voluntary approach, and avoid mandatory compliance measures?

Answer. Flexibility is key. Risk is temporal. Technology and its attendant workflows are evolving rapidly. Any measure that would reduce flexibility or slow down the ability to learn and innovate on how to best prevent cyber vulnerabilities would generate increased risk. Compliance measures exist today across all industries including the public sector and we are still vulnerable as a nation. So before we look at adding additional compliance measures, we need to determine why existing ones are not working.

In some cases this is because existing compliance measures are written in a way that requires the use of 20-year-old technology that doesn't work to prevent the issues. A great example of this is the variety of compliance requirements that evaluate security controls based on updates for signatures or the deployment of intrusion detection and response mechanisms. We need to remember that compliance does not equal commitment. Whatever approach is used (mandatory or voluntary), it needs to foster commitment to improving cyber risks through better prevention vs. the current approach of reaction and response. We witness every day proof that the current approach is not working to prevent these risks. More alarming, though, is the continued promotion of the current approach by many in the security industry that profit from the growing manifestation of cyber risks and the continued maintenance of this cycle of reaction and response through to currently outlined compliance measures. These measures must be updated to include newer technologies that are better suited to reduce cyber risk.

Question 3. The cybersecurity of the Internet of Things must be a top priority. Many of the devices in the Dyn attack last year were manufactured and located outside the U.S. How can we address cybersecurity risks from an international perspective? Given these devices provide a significant benefit to our economy, how do we also ensure American innovators are not at a competitive disadvantage in the global marketplace?

Answer. While location creates some potential level of risk, that is not the core contributor to our risk issue. The risk we are faced with today and in the future is caused by the way that these devices and applications are designed, developed, implemented, and maintained. Any device that executes code has the potential to execute malicious code. So, as a nation we must do a better job of advancing our efforts around having stronger security development life-cycle and privacy-by-design to prevent vulnerabilities in the creation of technology. This needs to be done nationally as well as internationally. We also need to encourage organizations as well as consumers to use security technologies that can prevent these risks with a high degree of efficacy and with a level of efficiency that does not degrade the computing experience. We need to attack the primary driver of our current and future cyber risks—the execution of malicious code on these devices. If we do these things our risks will be dramatically lower and we will unleash innovators to use computing to generate new opportunities for the Nation. The current reactive approach carries with it a growing risk penalty that makes us so vulnerable that it puts us at a global disadvantage. If we approach this correctly with a continuous focus on proactive prevention as much as possible, we will have the competitive advantage in the global marketplace because we will get a risk reduction dividend that will pay us back generously.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. EDWARD MARKEY TO
MALCOLM HARKINS

Question. The Federal Government relies on Internet of Things devices and could bear a heavy burden if these devices are breached by a cyberattack. To align security incentives and promote cybersecurity, should contractors and vendors selling Internet of Things devices to the Government be required to bear their financial responsibility in the event of a material breach through mechanisms like cyber insurance?

Answer. As I mentioned in my testimony, any device that executes code has the potential to execute malicious code. Responsibility for breaches should be recognized as a shared responsibility that includes the creator of the technology, the purchaser of the technology, and the user of the technology. So any responsibility needs to be evaluated from a few perspectives to assess potential financial “liabilities.” And that assessment needs to also understand that the potential for risk cannot be fully eliminated. However, those risks can be substantially reduced through preventative controls, and damage can be managed with the appropriate reactionary controls of detection and response.

Technology Creator Responsibilities

- (1) The creator of the technology should have an adequate security development lifecycle and privacy-by-design effort in place to as best as possible prevent a vulnerability that could generate a material or significant risk.
- (2) The creator of the technology should have an adequate response capability to effectively and efficiently mitigate a product vulnerability if one is found.

Purchaser/User of Technology Responsibilities

- (1) The organization who bought and deployed the technology should have an adequate set of internal controls (security technology and processes) that are implemented to substantially prevent the potential for a breach. This would include the evaluation of potential risks with the technology prior to its purchase and the evaluation and implementation of controls needed to mitigate those risks.
- (2) The organization that bought and deployed the technology should also have an adequate emergency response capability should the preventative controls fail to adequately manage the damage that could occur.

We are at a point in time where our lives and society have a growing digital dependence. Digital risk management requires a level of shared digital responsibility to prevent these risks to the best of our abilities. Some aspects of this risk can and should be handled through financial mechanisms like insurance. Insurance would only mitigate financial expenses after the fact from the resulting liability on either the creator or purchaser of technology. However, we need to realize that this would still be a reactionary approach focused on financial remuneration. It would also not deal with the full repercussions of a material breach such as those still being experienced following the breach at the Office of Personnel Management (OPM). That breach not only affected our national security and may well affect it for years to come, but it has a potential material impact on the lives of the individuals and families whose personal information was taken. The future Internet of things devices—if not designed, developed, implemented, and maintained properly—could have even more devastating implications that no form of financial remuneration could address.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TAMMY DUCKWORTH TO
MALCOLM HARKINS

Question 1. To all of the Witnesses, beyond standards and frameworks, from an industry perspective, what are the top three to five best practices you’ve identified to protect critical infrastructure that enables companies and governments to enact proactive measures instead of just focusing on the response to threats or disasters? Specifically, I want to know how we move from reaction to proaction.

Answer. Best practices to move from reaction to proaction include the following:

- (1) Strong security development lifecycle and privacy-by-design in the creation and implementation of technology.
- (2) Responsible vulnerability disclosure by any organization or individual who identifies a vulnerability.
- (3) Relentless focus on the preventing the execution of malicious code on all devices, because it is the primary driver of the cyber risk cycle.

- (4) Routine transparency within an organization to its executives and stakeholders on the state of security for the technology they use for internal operations as well as the technology they create for use by customers.
- (5) Demonstrating a culture of continuous improvement on how to identify risk and proactively prevent its cause.

Question 2. As this committee moves forward in the 115th Congress, we are considering oversight and legislation within the committee's jurisdiction of science, technology, transportation and the critical infrastructure that supports them. For all the witnesses in closing, what should this committee keep in mind in order to help make sure we're developing the framework for infrastructure that is proactive, resilient and lasting as cyber threats continue to evolve?

Answer. Security is a journey with no finish line. It's a continual, relentless pursuit as technology evolves along with the potential risks. As a nation, we have the capability to do a better job than we have done to date. Leveraging cutting-edge artificial intelligence and machine learning, Cylance has shown we can create a demonstrable and sustainable bend in the curve of cyber risk. By applying artificial intelligence (AI) and machine learning to the identification of malicious code, our flagship product CylancePROTECT offers future-proof prediction and prevention of the most advanced threats in the world, including advanced persistent threats, zero-days, and exotic exploitation techniques never before seen.

CylancePROTECT also guards from everyday viruses, worms, ransomware, spyware/adware, Trojan horse attacks and spam. The problem with legacy security solutions that are the common control in organizations today is that adversaries can continually evolve their techniques and tactics to bypass them, leaving enterprises exposed to attacks. This means that traditional solutions are reactive in nature and rely on a constant stream of "signature updates" that tell these solutions what type of files to look for after an attack was successful on some other system; these are called "zero-day" attacks.

Traditional security solutions are built around a basic set of rules and signature files that are costly and high risk because they require a zero-day "sacrificial lamb" before they can create the ability to block an attack. This means it is not possible to identify a new threat until after the damage is done on at least one system so that the malicious software can be studied and "fingerprinted." But CylancePROTECT is different—it can identify and defuse even never-before-seen attacks prior to execution. This means that we can stop new variations of attacks without a zero-day sacrificial lamb. Our AI-based solution is flexible and can support new generations of technologies such as "internet of things" devices and many others.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO
HON. ERIC ROSENBAUGH

Question 1. In your testimony, you noted that China is facilitating the growth of its "fintech" sector through a permissive regulatory environment. You further observed that Congress must clarify key regulatory issues in the United States. What barriers inhibit American competitiveness and economic growth in emerging fields like AI and blockchain? Please provide specific examples.

Answer. Regulatory uncertainty blocks experimentation and innovation by fintech firms, including in relation to digital currencies and blockchain technology. The UK Financial Conduct Authority's "regulatory sandbox" provides an example for how regulators can facilitate innovation, while maintaining consumer protections. The FCA grants fintech firms temporary approval to test their innovations, and exempts them from certain regulatory penalties, provided appropriate consumer safeguards are in place.

Another barrier to fintech innovation in the U.S. is that fintech firms are largely regulated on a state-by-state basis (unlike the incumbent banking and securities firms, which are largely federally regulated). This increases the cost and complexity of regulatory compliance, and inhibits firms' ability to scale their innovations across the country.

Regulatory overlap is also an impediment to the development and commercial adoption of AI. For example, autonomous vehicles must comply with different regulations in different states, which increases the costs of developing this technology, and raises barriers to entry for new firms. The commercial applications for AI cross myriad sectors—including transport, finance, and healthcare. Multiple regulatory agencies will need to develop AI expertise, and collaborate on uniform Federal standards, if they are to prevent regulation from constricting innovation.

Question 2. I was pleased to hear that the emerging technologies discussed at the hearing have the potential to create new jobs and build a well-trained cybersecurity workforce. In my home state of South Dakota, Dakota State University is helping to meet this demand by doubling enrollment in its cybersecurity program in the last five years, serving as a major participant in the National Science Foundation's CyberCorps program, and hosting GenCyber camps for high school girls.

a. What steps should American educational institutions take to encourage more students to choose cyber careers?

Answer. Encouraging socio-economic diversity is key to building the cybersecurity workforce of the future. Educational institutions should take steps to ensure that they are marketing cybersecurity offerings to a broad audience. Additionally, cybersecurity courses should not just be an option for new starters. Educational pathways that credit prior learning and professional experience will make it easier for professionals to change careers.

b. How can we promote the development of entry-level cybersecurity education using emerging technology tools? How can we also promote education in higher skill levels in this field?

Answer. The development of the cyber workforce should not be limited to higher education only. "Cyber apprenticeships," which could be delivered via flexible online courses, offer an alternative with lower financial barriers to entry than a bachelor's degree, and may increase diversity in the field.

To encourage the development of highly-skilled cyber workers, Federal Government employers, including the Department of Defense and Intelligence Community, should increase flexibility to support the careers of "citizen soldiers," who blend careers of government service and private sector work. In the Department of Defense, we significantly expanded the role of the National Guard in the National Cyber Mission Force in order to improve the Department's ability to attract, train and retrain high-end cyber operators. Government training provides an important pipeline for highly skilled cyber workers—even those who leave government can benefit the broader U.S. economy.

Question 3. Both technologies and threats are continually evolving. This Committee has passed significant, bipartisan legislation to advance voluntary, public-private collaboration on cybersecurity, as well as research and workforce development. For example, the Cybersecurity Enhancement Act of 2014 authorized the process for the NIST Framework for Improving Critical Infrastructure Cybersecurity. The NIST framework employs a flexible, risk-management approach that the private sector and security experts have praised. Do you believe that cybersecurity policy, especially in the context of the emerging fields we discussed at the hearing, should maintain a flexible, voluntary approach, and avoid mandatory compliance measures?

Answer. The NIST Cybersecurity Framework is a valuable tool for identifying and managing cybersecurity risks, and is a strong example of the benefits of public/private collaboration. The Framework has been a focal point for the development of legal standards and an improved insurance market for cyber risk. The Framework's flexible approach yields two key advantages: (1) it can be adopted by organizations regardless of size and business sector; and (2) it can evolve with changes in technology and threats.

However, a purely voluntary approach to compliance has not prompted the behavior changes needed to improve the Nation's cybersecurity. Recent high-profile hacks have demonstrated that poor cybersecurity will result in expensive litigation and CEOs losing their jobs. These trends will encourage investment in improved cybersecurity. That said, the strategic importance of this issue should compel congressional leaders to not passively wait for voluntary adoption of a private-sector derived cybersecurity framework. We cannot sit and watch while Americans suffer the strategic and economic consequences. Accordingly, at least in some sectors, compliance should be mandatory and it should be a baseline standard for Federal Government contractors.

Question 4. The cybersecurity of the Internet of things must be a top priority. Many of the devices in the Dyn attack last year were manufactured and located outside the U.S. How can we address cybersecurity risks from an international perspective? Given these devices provide a significant benefit to our economy, how do we also ensure American innovators are not at a competitive disadvantage in the global marketplace?

Answer. The United States government must take a much more active role in disrupting and dismantling "botnets"—networks of infected devices which are used to conduct cyberattacks such as the 2016 distributed denial of service attack against Dyn. Key national security organizations, led by the FBI and Department of Justice with the Department of Defense in support when needed, should work very closely

with private sector telecommunication companies and international partners, to neutralize botnets by blocking traffic between the malicious operator and infected devices and using more active defensive measures.

Additionally, all international ISPs have a responsibility to ensure the security and integrity of their networks, including by acting to block malicious traffic where they become aware of an attack.

Mandating product features or imposing product liability on the manufactures or distributors of Internet of things devices would be practically difficult from a legal perspective and also has the potential to handicap American cybersecurity firms. However, if producers of IoT devices continue to sacrifice cybersecurity—only to improve profit margins—the FCC should seriously consider regulation that ensures security is designed into IoT devices by default.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BILL NELSON TO
HON. ERIC ROSENBAACH

Question. Our election system is highly decentralized, but about 80,000 votes in three states decided the last presidential election. Therefore, if Russian state actors wanted to try to influence our elections again, they could conceivably do so by targeting a limited number of voting precincts.

Mr. Rosenbach, could Russia have the capability to influence future elections by targeting a relatively small number of votes?

Answer. Russia has both the capability and demonstrated intent to manipulate an election outcome by targeting only a relatively small number of votes or voting precincts. In practice, the complexity of the U.S. electoral system, and unpredictability of which particular votes will matter most to an election outcome, would make this kind of manipulation difficult.

The most serious problem is Russia's demonstrated willingness to conduct cyberattacks, in conjunction with effective information operation campaigns, against civilian targets, including our democratic institutions. Protecting these institutions must be among the United States' most vital national interests. We simply cannot allow adversaries, including but not limited to Russia, to have the perception that they can conduct attacks of this nature with impunity. The U.S. is yet to react to any cyberattack with a response that is visible, serious and will deter future cyberattacks against our democratic institutions. We must bolster our deterrence posture to ensure our democratic institutions and future elections are protected.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. EDWARD MARKEY TO
HON. ERIC ROSENBAACH

Question. The Federal Government relies on Internet of Things devices and could bear a heavy burden if these devices are breached by a cyberattack. To align security incentives and promote cybersecurity, should contractors and vendors selling Internet of Things devices to the Government be required to bear their financial responsibility in the event of a material breach through mechanisms like cyber insurance?

Answer. The Federal Government is only a small market for Internet connected devices. If it sought to impose onerous contractual liability standards on vendors, there is a risk that vendors would not be willing to sell to the government, or would charge significantly higher prices.

The government can best mitigate the cybersecurity risks posed by Internet of Things devices by ensuring that government networks follow appropriate procurement and network security processes. For example, the malware used in the 2016 Dyn denial of service attack accessed devices by using default usernames and passwords that had not been changed by users. This is basic cyber hygiene that all cybersecurity managers in the U.S. Government should address as standard practice.

Additionally, the government has a key role to play in helping the private sector to respond to attacks which use Internet of Things devices, particularly those commissioned by state adversaries. Responding to these types of attacks requires significant resources and engagement with international partners.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TAMMY DUCKWORTH TO
HON. ERIC ROSENBAUGH

Question 1. To all of the Witnesses, beyond standards and frameworks, from an industry perspective, what are the top three to five best practices you've identified to protect critical infrastructure that enables companies and governments to enact proactive measures instead of just focusing on the response to threats or disasters? Specifically, I want to know how we move from reaction to proaction.

Answer. First, to be proactive about the defense of critical infrastructure, we must bolster the US' deterrence posture regarding state-sponsored cyberattacks.

Second, the Intelligence Community plays a key role in proactively identifying plans for attacks through the collection of intelligence abroad. To assist intelligence agencies to identify and prevent cyberattacks, we need clear channels of communication between industry and government, as well as liability protection for information-sharing.

Third, the government can assist industry by testing the security and resilience of critical infrastructure systems. For example, the Washington State National Guard conducts "red team" exercises to search for vulnerabilities in state networks, and to test cyber-emergency responses. This practice has been adopted in a number of other states, and could be adopted further.

Finally, the NIST Cybersecurity Framework sets out important best practices for businesses involved in critical infrastructure, but we need to move beyond voluntary compliance. The government can establish and leverage incentives to promote adoption of the NIST framework, which could for example include technical assistance, regulatory streamlining, grants or liability protection for complying businesses. At least for some sectors, compliance with the NIST framework should be mandatory.

Question 2. As this committee moves forward in the 115th Congress, we are considering oversight and legislation within the committee's jurisdiction of science, technology, transportation and the critical infrastructure that supports them. For all the witnesses in closing, what should this committee keep in mind in order to help make sure we're developing the framework for infrastructure that is proactive, resilient and lasting as cyber threats continue to evolve?

Answer. To meet the current and future challenges of cybersecurity, the U.S. must continue to be on the leading edge of technological development. This is not just in our economic interest; it is a security imperative. Technological competitiveness can be supported in three ways.

First, the U.S. Government should invest in and be an early adopter of new technologies that will aid cyber defense.

Second, Congress and state legislatures must ensure that existing regulations designed in the pre-internet age do not obstruct the development of new technologies.

Third, we must ensure that new laws designed to protect our Nation's critical infrastructure do not inadvertently stifle innovation. Laws and regulations must be flexible, and designed to evolve in response to changing technological opportunities, vulnerabilities, and adversaries. They will therefore need to be informed by broad and ongoing consultation with industry.

This page intentionally left blank.

